Operation/Reference Guide

NXD-700Vi

7" Modero® Wall/Flush Mount Touch Panel with Intercom

Touch Panels

Last Revised: 4/1/2011

AMX Limited Warranty and Disclaimer

This Limited Warranty and Disclaimer extends only to products purchased directly from AMX or an AMX Authorized Partner which include AMX Dealers, Distributors, VIP's or other AMX authorized entity.

AMX warrants its products to be free of defects in material and workmanship under normal use for three (3) years from the date of purchase, with the following exceptions:

- Electroluminescent and LCD Control Panels are warranted for three (3) years, except for the display and touch overlay components are warranted for a period of one (1) year.
- Disk drive mechanisms, pan/tilt heads, power supplies, and MX Series products are warranted for a period of one (1) year.
- AMX lighting products are guaranteed to switch on and off any load that is properly connected to our lighting products, as long as the AMX lighting products are under warranty. AMX also guarantees the control of dimmable loads that are properly connected to our lighting products. The dimming performance or quality there of is not guaranteed, impart due to the random combinations of dimmers, lamps and ballasts or transformers.
- AMX software is warranted for a period of ninety (90) days.
- Batteries and incandescent lamps are not covered under the warranty.
- AMX AutoPatch Epica, Modula, Modula Series4, Modula CatPro Series and 8Y-3000 product models will be free of defects in materials and manufacture at the time of sale and will remain in good working order for a period of three (3) years following the date of the original sales invoice from AMX. The three-year warranty period will be extended to the life of the product (Limited Lifetime Warranty) if the warranty card is filled out by the dealer and/or end user and returned to AMX so that AMX receives it within thirty (30) days of the installation of equipment but no later than six (6) months from original AMX sales invoice date. The life of the product extends until five (5) years after AMX ceases manufacturing the product model. The Limited Lifetime Warranty applies to products in their original installation only. If a product is moved to a different installation, the Limited Lifetime Warranty will no longer apply, and the product warranty will instead be the three (3) year Limited Warranty.

All products returned to AMX require a Return Material Authorization (RMA) number. The RMA number is obtained from the AMX RMA Department. The RMA number must be clearly marked on the outside of each box. The RMA is valid for a 30-day period. After the 30-day period the RMA will be cancelled. Any shipments received not consistent with the RMA, or after the RMA is cancelled, will be refused. AMX is not responsible for products returned without a valid RMA number.

AMX is not liable for any damages caused by its products or for the failure of its products to perform. This includes any lost profits, lost savings, incidental damages, or consequential damages. AMX is not liable for any claim made by a third party or by an AMX Authorized Partner for a third party.

This Limited Warranty does not apply to (a) any AMX product that has been modified, altered or repaired by an unauthorized agent or improperly transported, stored, installed, used, or maintained; (b) damage caused by acts of nature, including flood, erosion, or earthquake; (c) damage caused by a sustained low or high voltage situation or by a low or high voltage disturbance, including brownouts, sags, spikes, or power outages; or (d) damage caused by war, vandalism, theft, depletion, or obsolescence.

This limitation of liability applies whether damages are sought, or a claim is made, under this warranty or as a tort claim (including negligence and strict product liability), a contract claim, or any other claim. This limitation of liability cannot be waived or amended by any person. This limitation of liability will be effective even if AMX or an authorized representative of AMX has been advised of the possibility of any such damages. This limitation of liability, however, will not apply to claims for personal injury.

Some states do not allow a limitation of how long an implied warranty last. Some states do not allow the limitation or exclusion of incidental or consequential damages for consumer products. In such states, the limitation or exclusion of the Limited Warranty may not apply. This Limited Warranty gives the owner specific legal rights. The owner may also have other rights that vary from state to state. The owner is advised to consult applicable state laws for full determination of rights.

EXCEPT AS EXPRESSLY SET FORTH IN THIS WARRANTY, AMX MAKES NO OTHER WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. AMX EXPRESSLY DISCLAIMS ALL WARRANTIES NOT STATED IN THIS LIMITED WARRANTY. ANY IMPLIED WARRANTIES THAT MAY BE IMPOSED BY LAW ARE LIMITED TO THE TERMS OF THIS LIMITED WARRANTY. EXCEPT AS OTHERWISE LIMITED BY APPLICABLE LAW, AMX RESERVES THE RIGHT TO MODIFY OR DISCONTINUE DESIGNS, SPECIFICATIONS, WARRANTIES, PRICES, AND POLICIES WITHOUT NOTICE.

AMX Software License and Warranty Agreement

- LICENSE GRANT. AMX grants to Licensee the non-exclusive right to use the AMX Software in the manner described in this License. The AMX Software is licensed, not sold. This license does not grant Licensee the right to create derivative works of the AMX Software. The AMX Software consists of generally available programming and development software, product documentation, sample applications, tools and utilities, and miscellaneous technical information. Please refer to the README.TXT file on the compact disc or download for further information regarding the components of the AMX Software. The AMX Software is subject to restrictions on distribution described in this License Agreement. AMX Dealer, Distributor, VIP or other AMX authorized entity shall not, and shall not permit any other person to, disclose, display, loan, publish, transfer (whether by sale, assignment, exchange, gift, operation of law or otherwise), license, sublicense, copy, or otherwise disseminate the AMX Software. Licensee may not reverse engineer, decompile, or disassemble the AMX Software.
- ACKNOWLEDGEMENT. You hereby acknowledge that you are an authorized AMX dealer, distributor, VIP or other AMX authorized entity in good standing and have the right to enter into and be bound by the terms of this Agreement.
- INTELLECTUAL PROPERTY. The AMX Software is owned by AMX and is protected by United States copyright laws, patent laws, international treaty provisions, and/or state of Texas trade secret laws. Licensee may make copies of the AMX Software solely for backup or archival purposes. Licensee may not copy the written materials accompanying the AMX Software.
- TERMINATION. AMX RESERVES THE RIGHT, IN ITS SOLE DISCRETION, TO TERMINATE THIS LICENSE FOR ANY REASON UPON WRITTEN NOTICE TO LICENSEE. In the event that AMX terminates this License, the Licensee shall return or destroy all originals and copies of the AMX Software to AMX and certify in writing that all originals and copies have been returned or destroyed.
- PRE-RELEASE CODE. Portions of the AMX Software may, from time to time, as identified in the AMX Software, include PRE-RELEASE CODE and such code may not be at the level of performance, compatibility and functionality of the GA code. The PRE-RELEASE CODE may not operate correctly and may be substantially modified prior to final release or certain features may not be generally released. AMX is not obligated to make or support any PRE-RELEASE CODE. ALL PRE-RELEASE CODE IS PROVIDED "AS IS" WITH NO WARRANTIES.
- LIMITED WARRANTY. AMX warrants that the AMX Software (other than pre-release code) will perform substantially in accordance with the accompanying written materials for a period of ninety (90) days from the date of receipt. AMX DISCLAIMS ALL OTHER WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WITH REGARD TO THE AMX SOFTWARE. THIS LIMITED WARRANTY GIVES LICENSEE SPECIFIC LEGAL RIGHTS. Any supplements or updates to the AMX SOFTWARE, including without limitation, any (if any) service packs or hot fixes provided to Licensee after the expiration of the ninety (90) day Limited Warranty period are not covered by any warranty or condition, express, implied or statutory.
- LICENSEE REMEDIES. AMX's entire liability and Licensee's exclusive remedy shall be repair or replacement of the AMX Software that does not meet AMX's Limited Warranty and which is returned to AMX in accordance with AMX's current return policy. This Limited Warranty is void if failure of the AMX Software has resulted from accident, abuse, or misapplication. Any replacement AMX Software will be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer. Outside the United States, these remedies may not available. NO LIABILITY FOR CONSEQUENTIAL DAMAGES. IN NO EVENT SHALL AMX BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OF OR INABILITY TO USE THIS AMX SOFTWARE, EVEN IF AMX HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES/COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO LICENSEE.
- U.S. GOVERNMENT RESTRICTED RIGHTS. The AMX Software is provided with RESTRICTED RIGHTS. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph ©(1)(ii) of The Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs ©(1) and (2) of the Commercial Computer Software Restricted Rights at 48 CFR 52.227-19, as applicable.
- SOFTWARE AND OTHER MATERIALS FROM AMX.COM MAY BE SUBJECT TO EXPORT CONTROL. The United States Export Control laws prohibit the export of certain technical data and software to certain territories. No software from this Site may be downloaded or exported (i) into (or to a national or resident of) Cuba, Iraq, Libya, North Korea, Iran, Syria, or any other country to which the United States has embargoed goods; or (ii) anyone on the United States Treasury Department's list of Specially Designated Nationals or the U.S. Commerce Department's Table of Deny Orders. AMX does not authorize the downloading or exporting of any software or technical data from this site to any jurisdiction prohibited by the United States Export Laws.

This Agreement replaces and supersedes all previous AMX Software License Agreements and is governed by the laws of the State of Texas, and all disputes will be resolved in the courts in Collin County, Texas, USA. For any questions concerning this Agreement, or to contact AMX for any reason, please write: AMX License and Warranty Department, 3000 Research Drive, Richardson, TX 75082.

FCC Information

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received; including interference that may cause undesired operation.

Federal Communications Commission (FCC) Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy, and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC RF Radiation Exposure Statement

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed an operated with a minimum distance of 20 centimeters between the radiator and your body.

Table of Contents

Introduction

The NXD-700Vi is an incredibly versatile user interface, combining a sleek, compact size, Wall/Flush Mount flexibility and the ability to create a high quality digital home/office intercom network or to make/receive digital local, long distance and international telephone calls. Simply add the AMX SIP Communications Gateway (**FG2182-0x**) for calls that sound incredibly clear.

FIG. 1 NXD-700Vi

Common Application

At just 7 inches in size, the NXD-700Vi is perfect for wall/flush mount control of a variety of devices in bedrooms, bathrooms, kitchens, podiums and other surface mount locations.

Features

- 7" active-matrix TFT with 16:9 Aspect Ratio
- Screen Resolution (HV): 800 x 480 pixels with Anti-glare Overlay
- Display colors: 256 K (18 bit color depth)
- Intercom with VoIP technology
- Full duplex audio built-in speaker and microphone
- G.711 telephone-voice-quality sound (70 dB SPL @ 1 meter)
- Supports analog stereo audio, Composite Video and S-Video
- Composite/S-Video inputs via NXA-AVB/Ethernet Breakout Box
- 64 MB SDRAM / 512 MB Compact Flash Memory or more
- 802.11g WiFi for two-way network communications (optional)
- Two bezels included: with and without tactile buttons
- Motion Sensor and Light sensor

These Color Video (CV) panels display NTSC/PAL/SECAM video formats within variable sized windows. They include a built-in microphone, speaker, audio/headphone connector, and six NetLinx programmable pushbuttons (*available on NXD models only when mounted with included Button Trim Ring*).

Each panel is sold only as part of a kit which includes both a panel and an NXA-AVB/ETHERNET Audio/ Video Breakout Box (**FG2254-10**). This box facilitates the installation and distribution of video (either Composite or S-Video), data (via Ethernet), and audio to Modero touch panels located up to 200 feet (60.96 m) from the breakout box. NXD-700Vi panels are ideally suited for displaying full motion video and audio with overlay graphics for applications with demanding visual requirements.

NXD-700Vi Widescreen Video Touch Panel Kit	
NXD-700Vi (**FG2258-04K**)	7" Widescreen Color Video Wall Mount Touch Panel Kit (with buttons) (includes both an NXD panel and an NXA-AVB/ETHERNET A/V Breakout Box).

The NXD-700Vi panel (FG2258-04) is shipped, by default with a Trim Ring containing buttons, but the end user can later install the included Trim Ring without button openings.

Key features common to both panels include:

- NXD-700Vi panels are based on the latest display technology and support AMX's 4th generation (G4) graphics which provide higher brightness, richer colors, and deeper contrast. The new G4 graphics technology is supported by the latest AMX TPDesign4 Touch Panel Design program (**version 2.6 or higher**).
- NXD-700Vi panels display eye-catching images and full-motion video on a large 16:9 image format, while providing a wide 100-degree top-to-bottom viewing angle.
- NXD-700Vi panels feature a front panel light sensor, motion sensor, IR receiver and a Sleep/Setup Access combo button.
- NXD-700Vi panels support *AMX Computer Control*, which enables remote viewing and control of any networked computer directly from the panel. This gives the user the ability to launch digital music from a PC, cruise the Internet, check and respond to E-mail, open software files, and launch applications. Anything you can do on your PC can be accomplished through these panels.
- The wireless solution includes an NXA-WC80211GCF internal Wi-Fi card (**FG2255-07**) that allows the NXD-700Vi to communicate with a NetLinx Master via a standard 802.11g Wireless Access Point.
- NXD-700Vi panels feature programmable firmware that can be upgraded via either the Ethernet port, wireless interface card, or the mini-USB port.

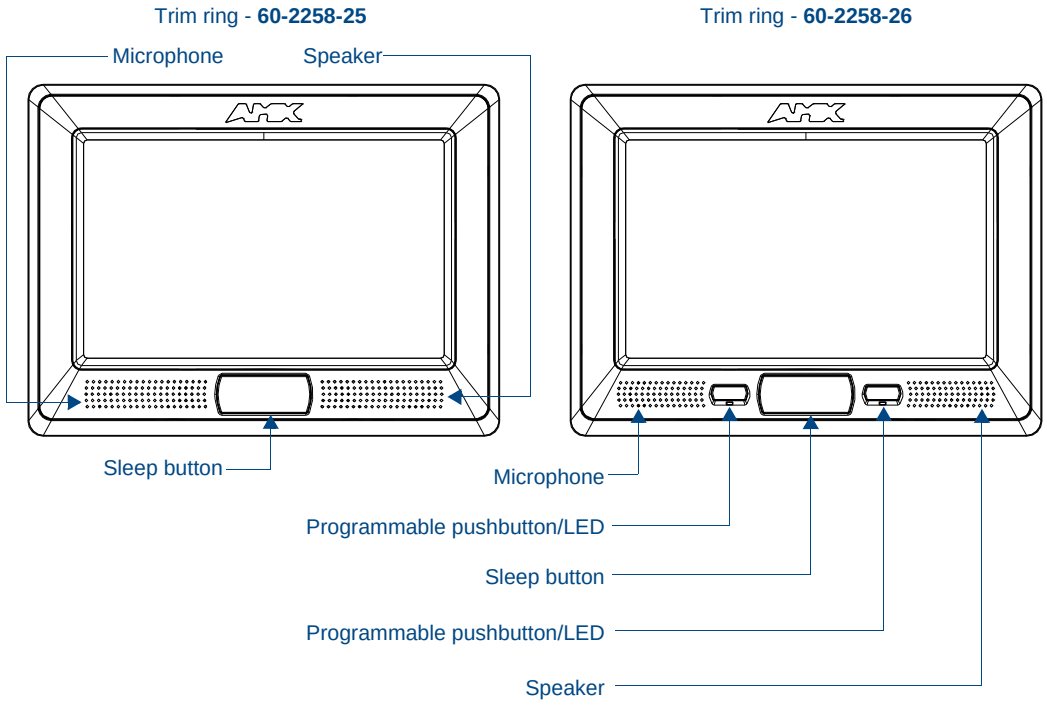


FIG. 2 NXD-700Vi (front views)

The NXD-700Vi comes with a standard silver bezel (FIG. 1), but the device is also available with the optional Mystique-style bezel (FIG. 3). The NXXD-700Vi may be ordered with the bezel already installed, or the bezel may be purchased separately to update the device to the latest Mystique style.

FIG. 3 NXD-700Vi with optional black Mystique-style bezel

Mystique Style Bezels	
Bezel	**Part Number**
NXD-700Vi 7" Modero Wall/Flush Mount Touch Panel with White Mystique-Style Bezel	FG2258-08K
NXD-700Vi 7" Modero Wall/Flush Mount Touch Panel with Black Mystique-Style Bezel	FG2258-07K
NXA-BEZ700-WH, White Bezel	FG2258-49
NXA-BEZ700-BL, Black Bezel	FG2258-48

NXD-700Vi Specifications

The following table outlines the specifications for the 7" Widescreen Modero panels.

Product Specifications	
Dimensions (HWD):	• NXA-RK7: metal rack-mount with black matte finish: (4 RU - rack units high) 6.97" x 19.0" x 0.50" (17.70 cm x 48.26 cm x 1.27 cm) • NXD-700Vi (with faceplate): 5.93" x 7.87" x 3.28" (15.06 cm x 20.00 cm x 8.33 cm) • CB-TP7 Conduit/Wallbox (*optional*): 5.47" x 7.23" x 3.40" (13.90 cm x 18.40 cm x 8.64 cm)
Power Requirements (stand-alone NXD-700Vi)**:**	• Constant current draw: 1.1 A @ 12 VDC (stand-alone) • Startup current draw: 1.6 A @ 12 VDC (stand-alone)
Memory (factory default):	• 64 MB SDRAM • 128 MB Compact Flash (upgradeable to 1 GB - factory programmed)
Weight (stand-alone):	• NXD-700Vi: 4.12 lbs (1.87 kg)
Certifications:	• FCC Part 15 Class B and CE • IEC60950
Panel LCD Parameters:	• Aspect ratio*:* 16 x 9 • Brightness (luminance): 350 cd/m^2 • Channel transparency: 8-bit Alpha blending • Contrast ratio: 200:1 • Display colors: 256 thousand colors (18-bit color depth) • Dot/pixel pitch: 0.19 mm • Panel type: TFT Color Active-Matrix • Screen resolution: 800 x 480 pixels (HV) @ 60 Hz frame frequency • Video format: NTSC, PAL, and SECAM • Viewing angles (100° total viewing angle): Vertical: + 50° (up from center) and - 50° (down from center)
Active Screen Area:	• 6.00" x 3.60" (15.24cm x 9.14cm)
IR Reception Angle:	• Horizontal: ± 50° (left and right from center) • Vertical: ± 30° (up and down from center)
Supported Audio Sample Rates:	• 48000Hz, 44100Hz, 32000Hz, 24000Hz, 22050Hz, 16000Hz, 12000Hz, 11025Hz, and 8000Hz.
Front Panel Components:	
Light sensor:	• Photosensitive light detector for automatic adjustment of the panel brightness (a dim room results in a dimmer LCD display, and a bright room results in a brighter LCD display). ***Note**: The light sensor can be adjusted via the Sensor Setup page (page 110).*
Motion sensor (PIR):	• Proximity Infrared Detector to wake the panel when the panel is approached. • Activation range: ± 45° (left and right from center) and ± 20° (up and down from center). ***Note**: This sensor can be adjusted via the Sensor Setup page (see page 110).*
IR Receiver:	• IR reception: 38 KHz IR frequency. • The IR receiver is located beneath the translucent Front Setup button. When an IR code is detected it is sent to the NetLinx Master as a push on the appropriate AMX IR channel. • IR receivers and transmitters on G4 panels share the device address number of the panel.

Product Specifications (Cont.)	
Side Panel Components:	
Front setup access button:	• Provides both access to the Setup and Calibration page and toggles the panel between a "sleep" or "wake" state. - When wired, "sleep" status means the backlight is Off. - When battery operated, wireless "sleep" status means the touch panel base is either Off or "suspended".
Microphone:	• Used for intercom applications (***requires the NXA-AVB/ETHERNET Breakout Box for analog communication***)
Speaker:	• Single 2 watt speaker
LEDs	• 2 blue LEDs (support On and Off) - Both the LEDs and pushbuttons are only available when using the default Button Trim Ring on the NXD panel.
Buttons	• 2 programmable pushbuttons
Mini-USB connector:	• 5-pin Mini-USB connector used for programming, firmware update, and touch panel file transfer between the PC and the target panel. ***Note**: When connecting the panel to PC using a CC-USB (or compatible) cable, be sure to power the panel On before attempting to connect the USB cable from the PC to the mini-USB port on the panel.*
Stereo Output connector:	• Stereo output through a 3.5mm mini-jack (for use with external speakers or headphones).
Ethernet 10/100 port:	• RJ-45 port for 10/100 Mbps communication. The Ethernet port automatically negotiates the connection speed (10 Mbps or 100 Mbps), and whether to use half duplex or full duplex mode. • NXD-700Vi panels communicate with the NetLinx Master using the ICSP protocol over Ethernet.
Ethernet 10/100 LEDs:	• LEDs show communication activity and connection information: **A**-activity - Yellow LED lights when receiving or transmitting Ethernet data packets. **L**-link - Green LED lights when the Ethernet cables are connected and terminated correctly.
USB connector:	• Type-A USB port can connect an external keyboard or mouse device for use with Virtual PC applications. ***Note**: External USB input devices (keyboard or mouse) must be plugged into the rear/side USB connector **before** the unit is powered-up. The panel will not detect these USB input devices until the unit cycles power.*
Audio/Video connector:	• RJ-45 connector for communication of differential audio/video signals to/from the touch panel (panel type dependant). This connector receives Composite video, Stereo (left/right) audio, and microphone audio. • Video is received via the NXA-AVB/ETHERNET Breakout Box. Configuring video windows for playback is done using TPDesign4. • In-bound audio (from the breakout box) gets directed to the speakers. • Out-bound audio is sent from the on-board microphone (on the front-panel). Selecting audio files for playback is configured through TPDesign4.
PWR connector:	• 2-pin 3.5 mm mini-Phoenix connector.
Button Assignments:	Button assignments can only be adjusted in TPD4 and not on the panels. • Button channel range: 1 - 4000 button push and feedback (per address port) • Button variable text range: 1 - 4000 (per address port) • Button states range: 1 - 256 (General Button; 1 = Off State, 2 = On State) • Level range: 1 - 600 (default level value 0-255, can be set up to 1-65535) • Address port range: 1 - 100

Product Specifications (Cont.)	
Operating / Storage Environment:	• Operating Temperature: 0° C (32° F) to 40° C (104° F) • Operating Humidity: 20% - 85% RH • Storage Temperature: -20° C (-4° F) to 60° C (140° F) • Storage Humidity: 5% - 85% RH
Included Accessories:	• Installation Kit for 7" NXD panels (**KA2258-02**) includes: - 2-pin 3.5 mm mini-Phoenix connector (41-5025) - Three Drywall clips (62-5924-05) and #6 - sheet metal screws - Four Phillips-head screws (#4-40 x 0.250 Black) • NXA-AVB/ETHERNET Breakout Box (**FG2254-10**): Provides video/audio distribution to the A/V panel over CAT5 cable (up to 200'/60.96m) and accepts either Composite or S-Video. *- Although the NXD-700Vi is only sold as part of a KIT configuration, the breakout box can be purchased as a separate accessory.* • Trim Ring with button openings (**60-2258-26**) • Trim Ring without button openings (**60-2258-25**)
Other AMX Equipment:	• CB-TP7 (**FG035-10**) - 7" metallic conduit box for Wall Mount installations. • CC-USB (Type A) to Mini-B 5-Wire programming cable (**FG10-5965**) • NXA-RK7 (**FG2904-53**) - RackMount kit for 7" Wall Mount touch panels (NXD panels only). Kit includes eight #10-32 screws and washers. • NXA-WC80211GCF Wireless Upgrade Kit (**FG2255-07**) - AMX 802.11G Compact Flash provides wireless Ethernet support • Upgrade Compact Flash (factory programmed with firmware): NXA-700CF256M, 256 MB COMPACT FLASH CARD (**FG2116-73**) NXA-700CF512M, 512 MB COMPACT FLASH CARD (**FG2116-74**) NXA-700CF1G, 1 G COMPACT FLASH CARD (**FG2116-75**)

It is recommended that firmware KIT files only be transferred over a direct USB or Ethernet connection and only when the panel is connected to a power supply. If battery power or wireless connection fails during a firmware upgrade, the panel flash file system may become corrupted.

NXD-700Vi Panels - Connector Layout

FIG. 4 shows the layout of the connectors (located on the rear of the base on the NXT and on the left side panel of the NXD panels).

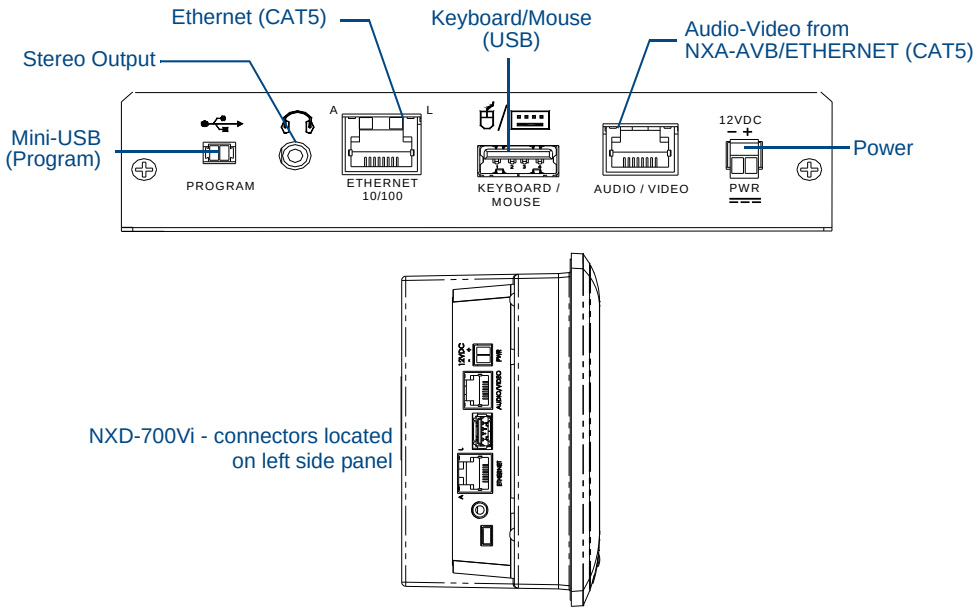


FIG. 4 Connector layout on the NXD-700Vi touch panels

NXA-AVB/ETHERNET Breakout Box

The NXA-AVB/ETHERNET Breakout Box (FIG. 5) is included as part of the NXD-700Vi Kit configuration (*panel and box*) but can be purchased as a separate accessory. This box facilitates the installation and distribution of video, data, and audio to Modero touch panels located up to 200 feet (60.96 m) from the AVB box. This unit accepts either Composite or S-Video from standard video devices.

This breakout box can be mounted on either a horizontal flat surface or within an equipment rack (by using an optional AC-RK Rack Kit).

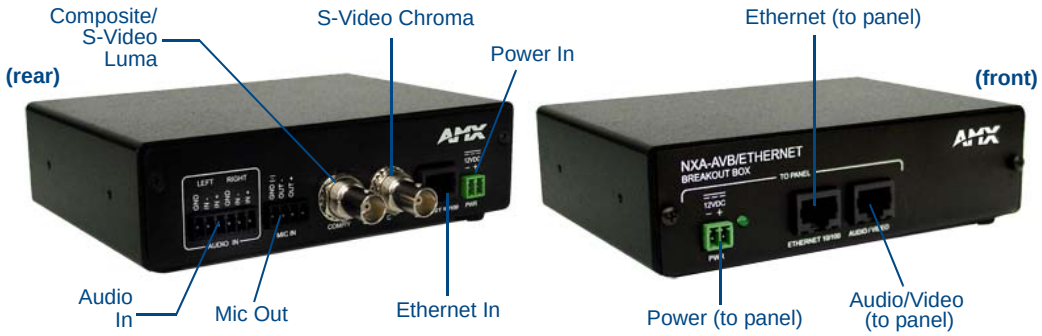


FIG. 5 NXA-AVB/ETHERNET Breakout Box (front and rear views)

Product Specifications

NXA-AVB/ETHERNET Product Specifications	
Dimensions (HWD):	• 1.50" x 5.55" x 4.88" (3.81 cm x 14.10 cm x 12.40 cm) • Width when attached to mounting ears: 6.65" (16.89 cm)
Power Consumption:	• 50mA (with audio/video input) • 23mA (with no audio/video) • Routed through NXA-AVB/Ethernet using a 12 VDC-compliant power supply
Certifications:	• FCC Part 15 Class B, CE, and EN60950
Features:	• Accepts either Composite or S-Video (***video-capable panels only***) • Provides audio distribution to the non-video touch panels over a CAT5 cable (up to 200 ft.) • Provides video/audio distribution to the video-capable touch panels over CAT5 cable up to 200 ft.(60.9 m)
Availability:	• This unit is included with CV5, CV7, CV10, NXD-700Vi, NXD-1000V,i and 1200V-Series Kit configurations
Front Components:	• 2-pin 3.5 mm Phoenix connector for power to the touch panel • Green LED provides an indication of power status • RJ-45 connector provides Ethernet signals to the touch panel • RJ-45 connector provides differential audio and video signals to the touch panel (panel type dependant)
Rear Components:	• 6-pin 3.5 mm Phoenix connector for in-bound (left/right channel) audio • 4-pin 3.5 mm Phoenix connector for out-bound (from microphone) audio • BNC connector (female) for Composite or Chroma (**for video-capable panels only**) • BNC connector (female) for luminance (**for video-capable panels only**) • RJ-45 connector for Ethernet input from the control system • 2-pin 3.5 mm Phoenix connector for in-bound power

NXA-AVB/ETHERNET Product Specifications (Cont.)	
Included Accessories:	• Two 2-pin Phoenix connectors (41-5025) • 4-pin Phoenix connector (41-5047) • 6-pin Phoenix connector (41-5063) • Rack Mount Kit (KA2250-40) with mounting bracket (62-2254-02)
Other AMX Equipment:	• AC-RK Accessory RackMount Kit (**FG515**) • Modero Table Top Cable (CA2250-50)

Installing the NXA-AVB/ETHERNET

A 12 VDC-compliant power supply can indirectly provide power to a Modero panel by routing power through the NXA-AVB/ETHERNET Breakout Box. FIG. 6 shows a sample wiring configuration using both an indirect or direct power connection for a video-capable Modero panel.

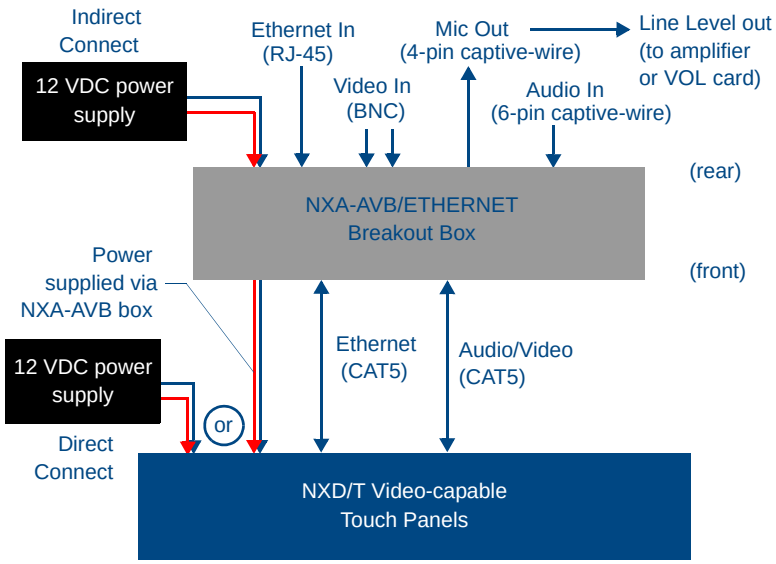


FIG. 6 Sample wiring configuration on video-capable panels using this breakout box

A 12 VDC-compliant power supply can also directly provide power through the unit to a target Modero panel. FIG. 7 shows a sample wiring configuration for a non-video capable Modero panel.

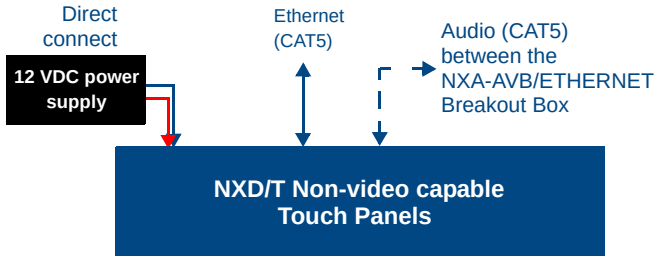


FIG. 7 Sample wiring configuration using non-video capable Modero panels

NOTE

The breakout box unit can be mounted on either a horizontal flat surface or into an equipment rack (by removing the front screws and attaching it to an optional AC-RK). The power supply being used on the NXA-AVB/ETHERNET is dependant on the power requirements of the target touch panel.

Use a standard CAT5 Ethernet cable to provide both communication and 10/100 network connectivity between the panel, NXA-AVB/ETHERNET, NetLinx Master, and the network.

Wiring the NXA-AVB/ETHERNET Connectors And Cables

The inputs and outputs on the breakout box are separated into front and rear connectors. The rear connectors are used to input external signals. The front connectors are used to communicate signals between the NXA-AVB/ETHERNET and a target Modero panel. FIG. 8 provides a layout of the wiring connection both into and from the breakout box.

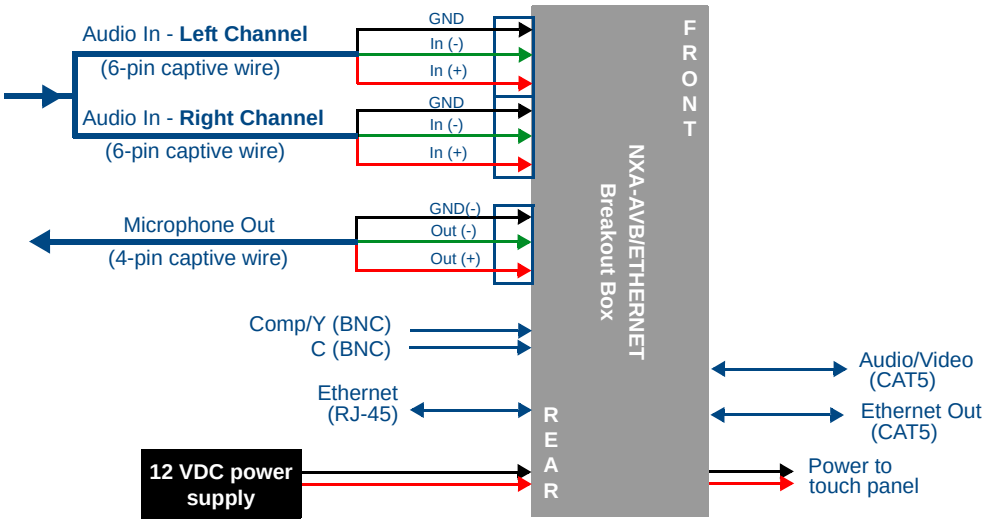


FIG. 8 NXA-AVB/ETHERNET Breakout Box connector wiring diagram

The rear-panel wiring connections are described below (from left to right):

- **AUDIO IN:** 6-pin mini-Phoenix connector, divided into left and right audio channels. Each channel is divided into GND, IN+, and IN- terminal cable connectors (2 sets of 3 for each channel).

  An example of this cable is to strip the ends of 2 RCA audio cables and insert them into their respective locations on the Audio In port.
  Either a balanced (+, -, and GND) or unbalanced (+ and GND) audio signal can be connected to this input.
- **MIC OUT:** 4-pin mini-Phoenix connector, divided into GND, OUT-, and OUT+ terminal connectors.

  An example of this cable is to strip the terminal ends of a 3.5mm mini-jack and insert them into their respective locations on the Mic Out port. This signal can be fed as a Line Level In to either an amplifier or an AMX VOL card.
  Either a balanced (+, -, and GND) or unbalanced (+ and GND) audio signal can be connected to this output.
- **Video In BNCs:** Feeds either Composite/S-Video Luma or S-Video Chroma signals into the NXA-AVB/ETHERNET. This feed is then redirected out to a Modero panel through the front Audio/Video CAT5 port.
- **ETHERNET:** RJ-45 connector routes data to the G4 touch panel through the front Ethernet port. These connections use a standard CAT5 Ethernet cable to provide communication between the target touch panel, breakout box, and NetLinx Master.
- **PWR:** 2-pin mini-Phoenix connector that connects to a 12 VDC-compliant power supply. This port can be used to provide power to a Modero panel by sending it through the NXA-AVB/ETHERNET (rear power connector through to the front power connector).

Wiring the NXA-AVB/ETHERNET for Unbalanced Audio

Most domestic audio equipment has unbalanced audio inputs and outputs. This means that the audio output (left, right, or mono) appears on a single wire, and is referenced to "0 V" or "Ground". Typical connectors used are RCA "phono" connectors, DIN plugs/sockets, and 0.25" (6.3mm) or 3.5mm jack plugs/sockets.

Unbalanced audio is adequate for most domestic environments and for line-level signals in a typical broadcast studio. Problems may occur if the signals are carried over long distances, especially if the source and destination have separate main supplies. Use the following wiring drawing (FIG. 9) to configure an unbalanced audio connection.

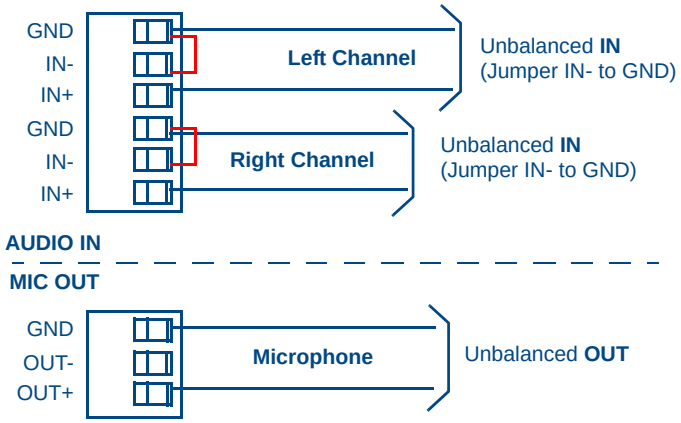


FIG. 9 Wiring the rear AUDIO IN and MIC OUT for use with Unbalanced Audio

When using unbalanced audio for the AUDIO IN connector (FIG. 9), the "-" and the "GND" terminals should be connected together and then connected to the GND of the unbalance audio signal. When connecting to an unbalanced audio input from the MIC OUT connector (FIG. 9), wire the "+" terminal to the signal input, and the "GND" terminal to the signal ground.

Wiring the NXA-AVB/ETHERNET for Balanced Audio

Professional audio equipment will often use balanced audio inputs and outputs, usually on 3-pin "XLR" connectors. A balanced audio signal consists of a pair of wires carrying the audio signal in anti-phase with each other (if one wire carries a positive voltage, the other carries an equal and opposite negative voltage).

The advantage of balanced audio over unbalanced audio is its ability to reject external interference added as the signal is carried over the wire. The receiving equipment takes the voltage difference between the two wires as the input signal. Interference will usually get added to both wires equally, and so gets cancelled by the receiving equipment.

The 3 wires used in a typical XLR lead are often referred to as Ground, Live (Hot) and Return (Cold). "Live" and "Return" carry the "in-phase" and "out-of-phase" versions of the audio respectively. The pins of the XLR plug/socket are as follows:

- X = Ground
- L = Live (Hot)
- R = Return (Cold)

When connecting the MIC OUT connector to a balanced audio input (FIG. 10), use all three audio terminals (+, -, and GND), then connect the "+" terminal to the "live" signal, the "-" terminal to the "return" signal, and the "GND" terminal to the ground signal.

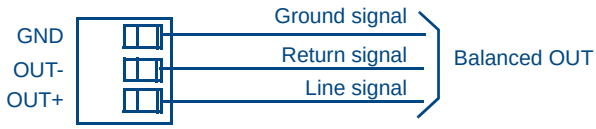


FIG. 10 Wiring the rear MIC OUT connector for use with Balanced Audio

NXD-700Vi Touch Panel Accessories

Overview

The following section outlines and describes the other AMX equipment available for these touch panels.

NXA-WC80211B/CF 802.11b Wireless Card (FG2255-03)

These touch panels can connect to a wireless network using an optional AMX 802.11b Wireless Interface Card shown in FIG. 1. This internal card is field-upgradeable within both models of panels.

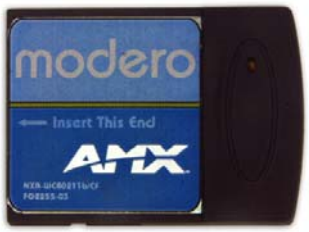


FIG. 1 NXA-WC80211B/CF Wireless Interface Card (WIC)

NOTE

This unit is certified and available for use in the United States (FCC), Canada (IC), Europe (CE) and Japan (TELEC).

The NXA-WC80211B/CF Wireless Interface Card works with compatible 802.11b Wireless Access Points such as the NXA-WAP200G. Please follow your particular Wireless Access Point's instruction manual for the correct procedures to setup either a secured or unsecured connection. The following table lists the specifications for the wireless interface card.

802.11b Wireless Interface Card Product Specifications	
Dimensions (HWD):	• 2.07" x 1.68" x 0.21" (52.56 mm x 42.80 mm x 5.57 mm)
Weight:	• 13.61 grams (0.030 lbs)
Description:	• 2.4 GHz Direct Sequence Spread Spectrum (DSSS) 802.11b 11M wireless PC card with detachable Antenna.
Features:	• Wired Equivalent Privacy (WEP) 64-bit and 128-bit data encryption • Diversity Antenna Connectors automatically select the best available signal • Supports infrastructure (communications to wired networks via Access Points), and roaming (standard IEEE 802.11b compliant)
Antenna:	• 2, Ceramic (Diversity Supported)
Certifications:	• FCC (United States) • IC (Canada) • CE (Europe) • TELEC (Japan)
Host Interface:	• Compact Flash Type I
Interoperability:	• Interoperable with Wi-Fi (WECA) certified products
LED Indicators:	• Power / Link activity
Modulation:	• DSSS, DBSK, DQSK, CCK
Network Standard:	• IEEE 802.11b
Number of Channels:	• 14
Operating Voltage:	• 5 / 3.3 V

802.11b Wireless Interface Card Product Specifications (Cont.)	
Operating Channels:	• 11 Channels (USA, Canada) • 13 Channels (Europe) • 14 Channels (Japan) • 4 Channels (France)
Operating Environment:	• Temperature: 0°C ~ 70°C (non-operating) and -15 ~ 80°C (storage) • Humidity (non-condensing): 5% ~ 95% RH
Power Consumption:	• TX power consumption: ≤ 265 mA • RX power consumption: ≤ 165 mA • Sleep Mode: 2 mA - 15 mA
Radio Data Rate:	• 1Mbps, 2Mbps, 5.5Mbps, 11Mbps, Auto Rate
Receive Sensitivity:	• @PER < 8% 11 Mbps: -83 dBm (max) 5.5 Mbps: -86 dBm (max) 2 Mbps: -89 dBm (max) 1 Mbps: -92 dBm (max)
RF Output Power:	• 15 dBm +/- 1 dBm • Channels 1 - 11 (North America)
Security:	• WEP 64,128 bit, WPA/TKIP
Wireless Restrictions:	• In R&TTE countries, such as France, the 802.11g frequency band is restricted to 2454 - 2483.5 MHz (2.4 - 2.4835 GHz) and a max power output of 100 mW EIRP outdoor.

NOTE

It is recommended that any upgrade of internal equipment be done simultaneously in order to reduce the risk of damage to internal components.

NXA-WC80211GCF 802.11g Wireless Card (FG2255-07)

These panels can also connect to a wireless network using the (optional) 802.11g Wi-Fi CF card. This internal WIC (FIG. 2) can be purchased separately as a Wi-Fi upgrade kit from AMX.

FIG. 2 NXA-WC80211GCF 802.11g wireless card

This interface card (**FG2255-07**) is a 2.4 GHz Wi-Fi LAN CF Card which upgrades a Modero panel's wireless RF capabilities from 802.11b to 802.11g. This card also provides the end-user with several new methods of wireless encryption and data security such as WPA and WPA2. In addition to being backwards compatible with 802.11b networks, this card is installable within all current MVP, NXD-700Vi, NXD-10000Vi, CV7, and CV10 panels. To fully utilize these newer wireless security features, this card must be used in tandem with the latest Modero firmware upgrade available at **www.amx.com**.

This card works with compatible 802.11b/g Wireless Access Points such as the NXA-WAP200G (*which uses a default SSID of **AMX***). Please follow your particular Wireless Access Point's instruction manual for the correct procedures to setup either a secured or unsecured connection. The following table lists the specifications for the NXA-WC80211GCF.

This upgrade kit requires that pre-existing panels first be removed from their current location (surface, wall or docking station) before an installer can access the internal circuit boards and upgrade a pre-existing 802.11b wireless CF card.

Only MVP panels require the use of a cardboard cutout (Mounting Template) to properly position the metal antenna plate onto the inner surface of the unit's rear plastic housing

NXD-700Vi, NXD-1000Vi, CV7, and CV10 panels only require locating the Compact Flash's metal cover plate on the main circuit board and then adhering the terminal antenna connector to that location using the included double-sided adhesive tape.

NOTE

If the CF metal cover plate is not present over the wireless card slot on a NXD-700Vi, NXD-1000Vi, CV7, or CV10 panel, you can use the adhesive tape to secure the terminal antenna to the surface of the new card (atop the product label).

The procedures for upgrading a CF card on an MVP is identical for both MVP-7500 and MVP-8400 panels. The procedures for upgrading/installing the new CF card are also similar across all referenced NXT panels and NXD panels as a group (differences arise from their housing).

NXA-WC80211GCF Specifications	
Dimensions (HWD):	• 0.22" x 1.68" x 2.40" (5.6 mm x 42.80 mm x 61.0 mm)
Weight:	• 19.50 grams (0.043 lbs)
Description:	• Wireless LAN Compact Flash Card with external PIFA antenna. • Features enterprise-class security such as WPA and WPA2 security.
Features:	• Compact Flash Type I form factor • Enhanced range and throughput • Features wireless security such as: WPA, WPA2 and WEP • Field-installable • Incorporates DSSS and OFDM radio technology • Operates at ISM frequency bands of 2.4 GHz, while providing data transfer speeds of up to 54Mbps. • Support for IEEE 802.11b and 802.11g • Supports Advanced Encryption Standard (AES) 64-bit and 128-bit data encryption, along with an Re4 encryption cipher (64/128-bit) • Supports authentication methods such as: EAP-FAST, EAP-LEAP, EAP-PEAP, EAP-TLS, and EAP-TTLS • Supports Wired Equivalent Privacy (WEP) 64-bit and 128-bit data encryption (known to the on-board firmware as Static WEP)
Antenna Type:	• External PIFA antenna (factory-installed)
Bus Interface:	• Compact Flash Type I
Certifications:	• FCC Part 15 Class B, CE, IC, TELEC, and Wi-Fi
Media Access Control Techniques:	• Using 802.11b DSSS communication: DBPSK @ 1 Mbps DQPSK @ 2 Mbps CCK @ 5.5 Mbps • Using 802.11g OFDM communication: BPSK @ 6 and 9 Mbps QPSK @ 12 and 18 Mbps 16-QAM @ 24 and 36 Mbps 64-QAM @ 48 and 54 Mbps

NXA-WC80211GCF Specifications (Cont.)	
Network Architecture:	• Infrastructure mode (Client-to-Access Point)
Operating Channels:	• Using 802.11b & g communication: - 04: (Ch 10 - 13) - France - 11: (Ch 1 - 11) - North America - 13: (Ch 1 - 13) - Europe ETSI - 13: (Ch 1 - 13) - Japan (802.11g) - 14: (Ch 1 - 14) - Japan (802.11b) ***Note**: To alter the card's default country code (North America), please contact an AMX Technical Support representative for detailed procedures and information.*
Operating Environment:	• Temperature: 0°C ~ 45°C (32°F to 113°F) (operating) and -20°C ~ 70°C (-4°F to 158°F) (storage) • Humidity: (non-condensing) 5% ~ 90% RH (operating) and (non-condensing) 5% ~ 95% RH (storage)
Operating Voltage:	• 3.3V + 5% I/O supply voltage
Power Consumption:	• @ 802.11b communication: - RX: 270 mA - TX: 435 mA - Standby: 240 mA • @ 802.11g communication: - RX: 270 mA - TX: 460 mA - Standby: 240 mA
Radio Data Rate:	• 802.11g compliant: 1, 2, 5.5, 11 (DSSS/CCK); 6, 9, 12, 18, 24, 36, 48, and 54 (OFDM) Mbps data rates
Radio Technology:	• Using 802.11b communication: DSSS (Direct Sequence Spread Spectrum)/CCK (Complementary Code Keying) • Using 802.11g communication: DSSS/CCK, OFDM (Orthogonal Frequency Division Multiplexing
Receiver Sensitivity:	• Using 802.11b communication @ FER<8%: 1 Mbps: -94 dBm (max) 2 Mbps: -93 dBm (max) 5.5 Mbps: -92 dBm (max) 11 Mbps: -90 dBm (max) • Using 802.11g communication @ PER <10%: 6 Mbps: -87 dBm (max) 9 Mbps: -86 dBm (max) 12 Mbps: -86 dBm (max) 18 Mbps: -84 dBm (max) 24 Mbps: -82 dBm (max) 36 Mbps: -78 dBm (max) 48 Mbps: -74 dBm (max) 54 Mbps: -72 dBm (max)
RF Frequency Ranges:	• Using 802.11b & g communication: Europe ETSI: 2.412 ~ 2.472 GHz France: 2.457 ~ 2.472 GHz Japan (802.11b): 2.412 ~ 2.484 GHz Japan (802.11g): 2.412 ~ 2.472 GHz North America: 2.412 ~ 2.462 GHz
Standard Conformance:	• IEEE 802.11b • IEEE 802.11g • IEEE 802.11e • IEEE 802.11i • Wi-Fi (WPA and WPA2)

NXA-WC80211GCF Specifications (Cont.)	
Transmit Output Power:	• 802.11b communication: 12 +-1 dBm (1, 2, 5.5, 11 Mbps) • 802.11g communication: 12 +-1 dBm (6, 9, 12, 18, 24, 36, 48, and 54 Mbps)
Wireless LAN Security:	• EAP-FAST • EAP-LEAP • EAP-PEAP • EAP-TLS • EAP-TTLS • WEP 64 & 128 • WPA-PSK
Touch Panel Compatibility:	• MVP-7500 (**FG5965-01**) • MVP-8400 (**FG5965-02**) • NXD-700Vi (**FG2258-04**) • NXD-1000Vi (**FGXXXXX**) • NXD-CV10 (**FG2259-02**) • NXT-CV10 (**FG2259-01/03**) • NXD-CV7 (**FG2258-02**) • NXT-CV7 (**FG2258-01**)
Included Accessories:	• Double-sided adhesive tape • Mounting Template cutout (62-2255-04) • NXA-WC80211GCF Installation Guide • Two Alcohol cleaning pads • Wireless CF card with wireless antenna
Other AMX Equipment:	• NXA-WAP250G Modero Wireless Access Point (**FG2255-50**) • Upgrade Compact Flash memory (factory programmed with firmware): NXA-CFSP128M - 128 MB compact flash card (**FG2116-36**) NXA-CFSP256M - 256 MB compact flash card (**FG2116-37**) NXA-CFSP512M - 512 MB compact flash card (**FG2116-38**) NXA-CFSP1GB - 1 GB compact flash card (**FG2116-39**)

NXA-CFSP Compact Flash (FG2116-7x)

Overview

Every NXD-700Vi Modero panel is shipped with a 128 MB Compact Flash card (NXA-CFSP).

If possible, upgrade the panel's internal components (Compact Flash or wireless interface cards) prior to installing or using the panel.

The NXA-CFSP Compact Flash card is factory programmed with specific panel firmware and can be upgraded to several sizes, up to 1GB:

Optional Compact Flash Upgrades	
• NXA-700CF256M, 256 MB COMPACT FLASH CARD	(**FG2116-73**)
• NXA-700CF512M, 512 MB COMPACT FLASH CARD	(**FG2116-74**)
• NXA-700CF1G, 1 G COMPACT FLASH CARD	(**FG2116-75**)

Upgrading the Compact Flash card in both panel types involves opening the panel enclosure/outer housing to access the internal circuit board, removing the existing card, replacing it, and then resecuring the panel enclosure, as described in the following section.

Installation and Upgrade of the Internal NXD Components

Overview

Upgrading the cards within the Wall Mount panel involves removing the rear plastic outer housing (back box), removing the existing card, replacing it, and then placing the back box back onto the NXD panel, as described in the following sections.

Step 1: Remove the existing NXD Outer Housing

1. Carefully detach all connectors from the side of the touch panel and remove the Faceplate from the front of the panel.
2. Place the LCD facedown on a soft cloth to expose the under-side of the unit (FIG. 3). This step helps prevent scratching of the LCD.

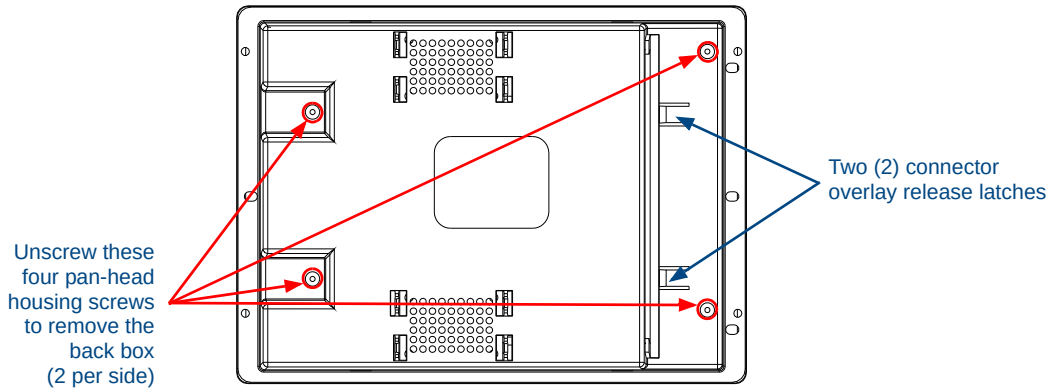


FIG. 3 Location of the attachment screws and connector overlay release latches on an NXD back box

3. Firmly press down on both connector overlay release latches (located in front of the connectors). *Pressing down releases the connector overlay from atop the connectors.*

NOTE

The overlay connector must first be released before the rear back box can be removed from the NXD-CV7/NXD-700Vi panel.

4. Gently slide the connector overlay away from the back box housing.
5. Unscrew the outer housing (back box) by using a grounded Phillips-head screwdriver to remove the two sets of pan-head Housing Screws, located on both sides of the housing (FIG. 3).

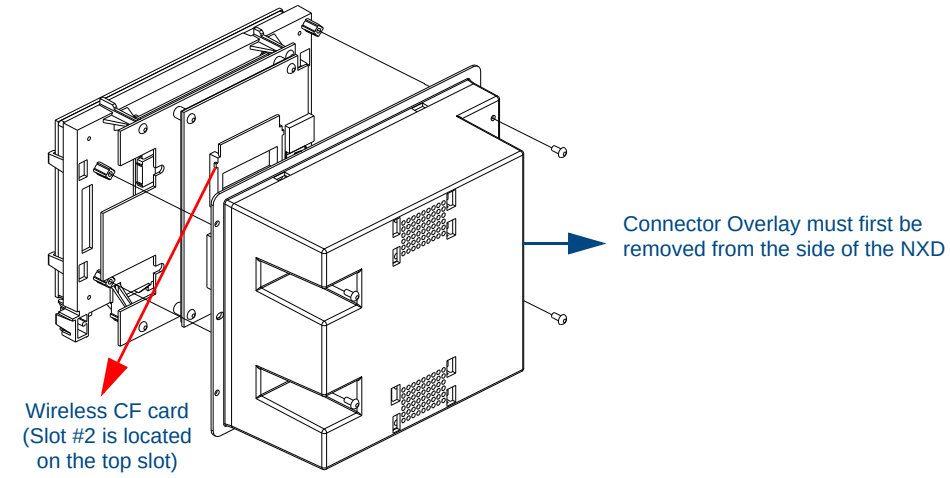


FIG. 4 Location of the wireless CF card connector on main board

6. Carefully lift-off the back box housing and angle it over to the side of the unit where the wires are connected to the circuit board.
7. Gently lay the back box to one side of the unit. This exposes the internal circuit board (FIG. 4). Take care not to place undue strain on the speaker cables.

Step 2: Install the new Compact Flash Memory card

1. Discharge any static electricity from your body by touching a grounded metal object and then locate the existing 128 MB Compact Flash card on the main board (FIG. 5).

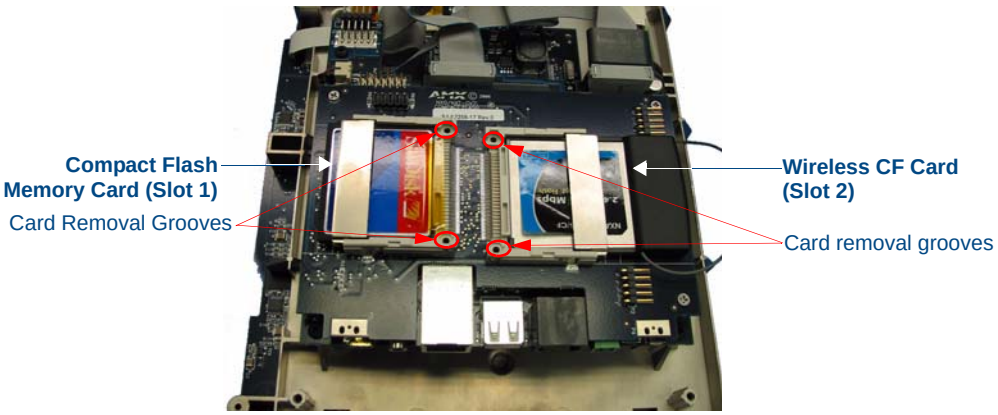


FIG. 5 Location and orientation of the card slots

2. Insert the tip of a grounded flat-head screwdriver into one of the card removal grooves (located on either side of the existing card), and gently pry the card out of the slot (FIG. 6). Repeat this process on the opposite card removal groove. This alternating action causes the card to "wiggle" away from the on-board connector pins.
3. Grip the old card by its sides and then carefully pull it out of the slot.
4. Remove the new CF memory card from it's anti-static bag.
5. Grip the sides of the new CF memory card and firmly insert it into slot opening (with the arrow facing towards the pins) until the contact pins are completely inside the flash card and it is then securely attached to the pin sockets.

6. To complete the upgrade process, either upgrade the remaining wireless card (Step 3) or close and re-secure the enclosure using the procedures in *Step 3: Close and Re-secure the NXD Panel Enclosure* section on page 23.

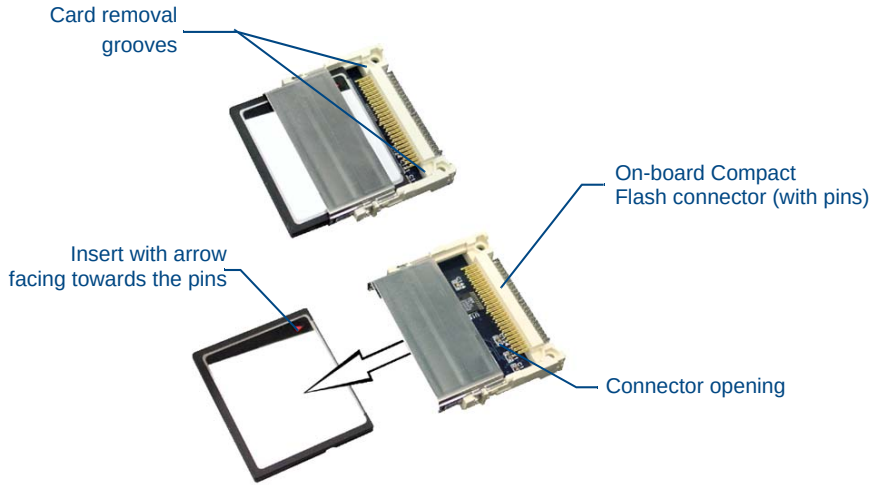


FIG. 6 Removing/installing a Compact Flash Memory card

NOTE

Any new internal card upgrade is detected by the panel only after power is cycled.

Step 3: Close and Re-secure the NXD Panel Enclosure

1. Gently place the outer housing back onto the panel and align the four pan-head Housing Screws holes along the edges of the outer housing.
2. Insert and secure the four pan-head Housing Screws back into their pre-drilled holes by using a grounded Phillips-head screwdriver.
3. Slip the connector overlay back into the connector opening by inserting the top of the overlay into the connector opening in an upwards direction.
4. Align the connectors to their respective locations and secure the overlay by pushing it towards the connectors until the overlay securely snaps back into the overlay release latches.
5. Re-install the faceplate back onto the panel. Refer to the *Installing the Button Trim Ring* section on page 26 for more detailed faceplate installation information.

Installation

Overview

NXD-700Vi panels are installed into either a pre-wall surface (using a CB-TP7 conduit/wallbox) or a solid surface (using either solid surface or drywall screws).

NOTE

It is recommended that if you are planning on upgrading your flash memory, you do so before beginning any panel installations.

Installing the No-Button Trim Ring

The NXD-700Vi panel is shipped from AMX with the default Button Trim Ring already installed. The unit is also shipped with an included Trim Ring containing no button openings (a No-Button Trim Ring) that allows you, if desired, to change the default configuration of the NXD panel Faceplate to that with no-button openings. In order to install this included No-Button Trim Ring, you must first remove the factory-installed default Button Trim Ring, the six small buttons, and associated two clear light pipes.

1. The Faceplate is secured to the panel with plastic latches. To remove the Faceplate, simply pull it away from the panel by gently tugging it outwards until the entire Faceplate comes away from the panel.
2. Turn the Faceplate over to expose the inside surface and view the Trim Ring latches (FIG. 7).
3. In a single motion, press down and then outwards on the three Trim Ring latches located along the top of the internal surface of the Faceplate to begin removing the Button Trim Ring. *Removing the Internal Faceplate from the panel exposes the pushbuttons and light pipes along the inside of the Internal Faceplate.*
4. Gently tug along the edges of the Button Trim Ring and work your way around the edges to remove it from the Faceplate (FIG. 7).

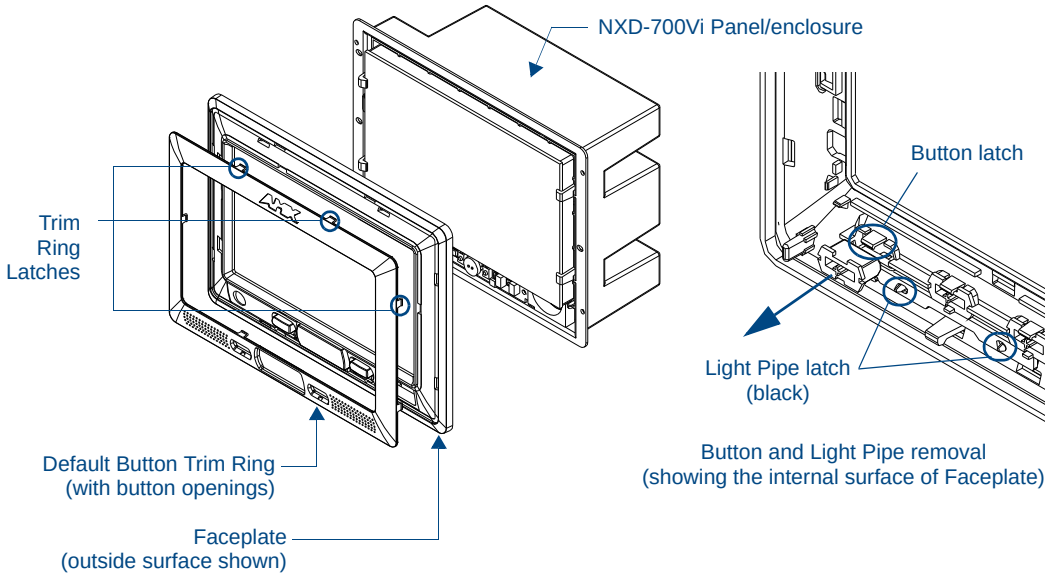


FIG. 7 Removing the default Button Trim Ring

5. From along the internal surface of the Faceplate, remove the six buttons by gently bending each Button latch up and pulling the button outwards.
6. Remove the pair of clear light pipe strips by bending the two black light pipe latches inwards and pulling out the strip.
7. Grasp the No-Button Trim Ring on both sides and fit it into the groove along the outside surface of the Faceplate (made available by the removal of the previous Trim Ring).
8. Gently insert the Trim Ring latches into their corresponding openings on the outer surface of the internal Faceplate (FIG. 8).

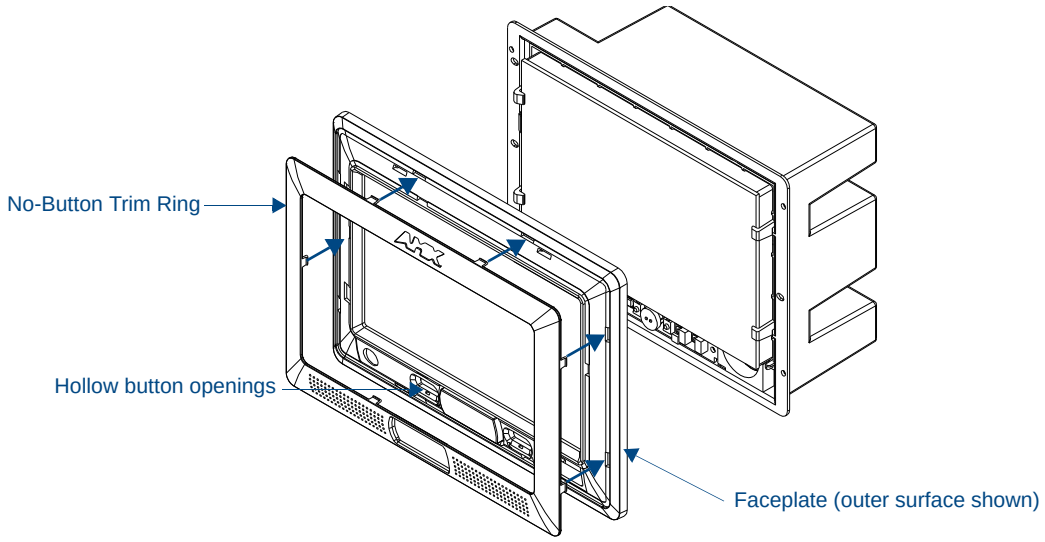


FIG. 8 Inserting the No-Button Trim Ring

9. Firmly press down around the No-Button Trim Ring until all of the latches are securely inserted into their openings on the Faceplate, and the No-Button Trim Ring is securely fastened. Verify the No-Button Trim Ring is firmly inserted onto the Faceplate and that there are no gaps between this Trim Ring and the outer surface of the Faceplate.
10. Place the Faceplate back onto the main NXD-700Vi unit. Make sure to align the Microphone, Light, and PIR Motion sensor locations on the main unit to their respective openings on the Faceplate assembly.

Installing the Button Trim Ring

The outer No-Button Trim Ring is secured to the Faceplate with plastic latches. In order to re-install the Button Trim Ring back onto an NXD panel which has had the default Button Trim Ring features removed; you must first remove the No-Button Trim Ring:

1. To remove the Faceplate, simply pull it away from the panel by gently tugging it outwards until the entire Faceplate comes away from the panel.
2. Turn the Faceplate over to expose the inside surface and view the Trim Ring latches.
3. In a single motion, press down and then outwards on the three Trim Ring latches located along the top of the internal surface of the Faceplate to begin removing the Trim Ring. *Removing the Internal Faceplate from the panel exposes the pushbuttons openings left from an earlier removal of the pushbuttons and LEDs.*
4. Gently tug along the edges of the No-Button Trim Ring and work your way around the edges to remove it from the Faceplate (FIG. 9).

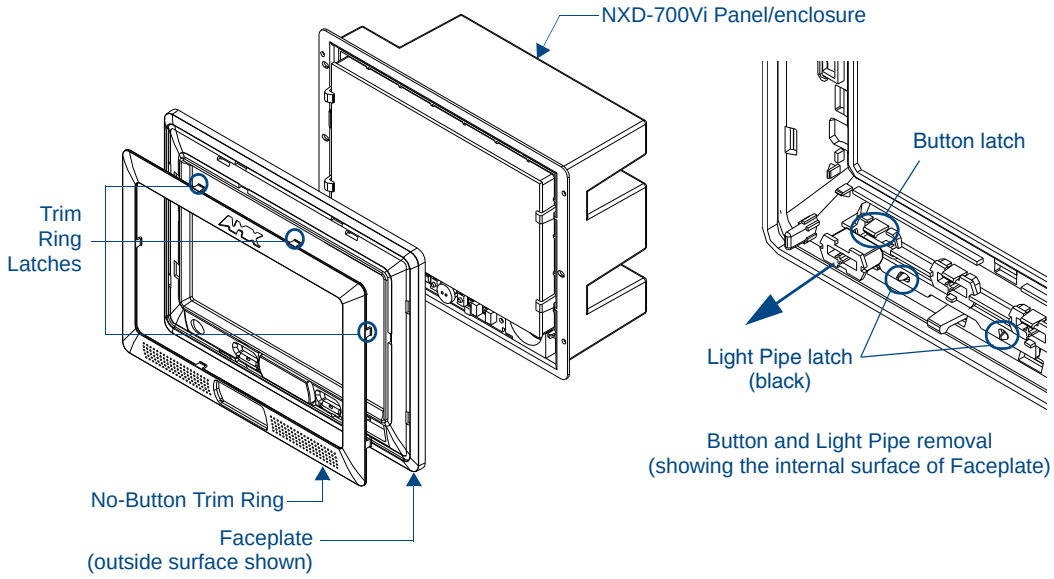


FIG. 9 Removing the No-Button Trim Ring

5. From along the internal surface of the Faceplate, install the six buttons by firmly inserting them into the button openings until the Button latch secures the button in place (FIG. 9).
6. Install the pair of clear light pipe strips by pushing light pipes over the two black light pipe latches.
7. Grasp the Button Trim Ring on both sides and fit it into the groove along the outside surface of the Faceplate (made available by the removal of the previous Trim Ring).
8. Gently insert the Button Trim Ring latches into their corresponding openings on the outer surface of the internal Faceplate (FIG. 10).

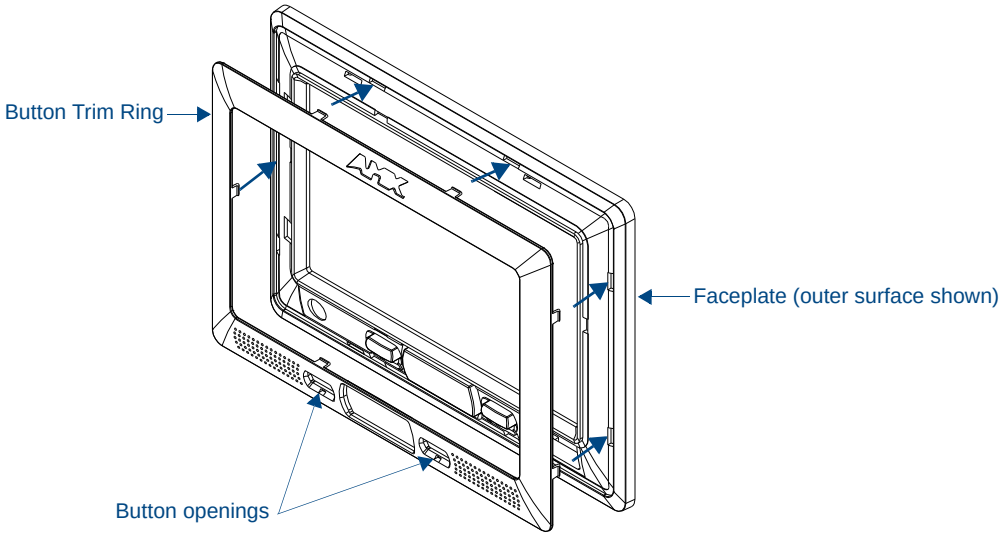


FIG. 10 Inserting the Button Trim RIng

9. Firmly press down around the Button Trim Ring until all of the latches are securely inserted into their openings on the Faceplate, and the Button Trim Ring is securely fastened. Verify the Button Trim Ring is firmly inserted onto the Faceplate and that there are no gaps between this Trim Ring and the outer surface of the Faceplate.
10. Place the Faceplate back onto the main NXD-700Vi unit. Make sure to align the Microphone, Light, and PIR Motion sensor locations on the main unit to their respective openings on the Faceplate assembly.

Pre-Wall Installation of the Conduit Box

Wall Mount panels (NXDs) are contained within an outer housing (back box). This back box is **not** removed when installing the NXD into a Conduit Box (CB-TP7). The back box is ***only*** removed to gain access for the replacement of the internal components.

WARNING

INSTALLER: LEAVE A GAP BETWEEN THE STUD AND CONDUIT BOX MOUNTING TABS TO ACCOMMODATE THE DRYWALL or SHEETROCK. This gap allows the installation of the drywall or sheetrock after the CB-TP7 Conduit Box has been installed.

The CB-TP7 is an optional metallic box that is secured onto a stud/beam in a **pre-wall** setting (*where no walls are present*). Installation procedures and configurations can vary depending on the installation environment. This section describes the installation procedures for the most common installation scenario. The most important thing to remember when mounting this conduit box is that the NXD-700Vi Mounting Tabs must lie flush against the outside of the sheetrock (FIG. 11).

- Refer to **SP-2258-02** for detailed installation dimensions.
- It is recommended that you cut out the surface slightly smaller than what is outlined in the installation drawings so that you can make any necessary cutout adjustments.
- The wiring knockouts on the left side will be used for the NXD-700Vi Wall Mount panel connectors, so always secure the conduit box to the stud using the Stud Mounting Holes on the right side of the box.

1. Rest the right Stud Mounting tabs onto the stud (keeping the knockouts on the left). **Be sure to leave enough of a gap between the stud and NXD Mounting tabs to accommodate the installation of the drywall or sheetrock after the conduit box has been mounted. Ultimately, the Mounting Tabs should lie flush against the outside of the sheetrock.**
2. Fasten the CB-TP7 conduit box to the stud through the holes on the right Stud Mounting tabs (FIG. 11), using either nails or screws.

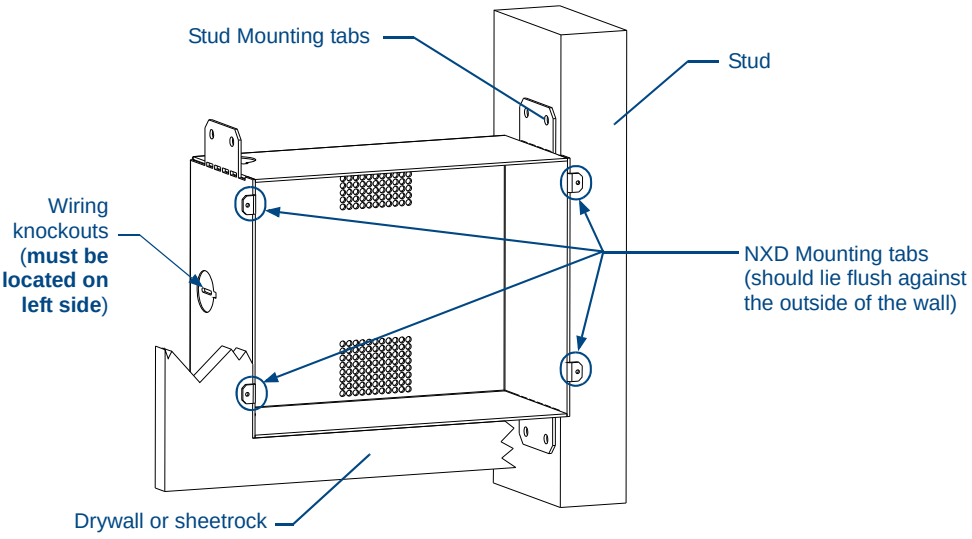


FIG. 11 CB-TP7 conduit box components

3. Remove the wiring knockouts from the left side of the conduit box (CB-TP7) (FIG. 11) to accommodate the cables being threaded through to the NXD touch panel.

NOTE

Remember that when mounting this conduit box, the NXD mounting tabs must lie flush against the outside of the sheetrock.

4. Thread the incoming power, RJ-45 audio/video, Ethernet, and USB wiring through the knockouts (***use of the left wiring knockouts are recommended with this installation***).
   Leave enough slack in the wiring to accommodate any re-positioning of the panel.
5. Install the drywall/sheetrock before inserting the main NXD unit into the CB-TP7.

Installation of an NXD Touch Panel

The NXD-700Vi can be installed either directly into the (optional) CB-TP7 or other solid surface environment using the two different mounting options: drywall clips or solid surface screws. The following sections describe mounting the touch panel directly into a pre-wall conduit box, a solid surface or drywall, and optional NXA-RK7 Rack Mount Kit.

Installing the NXD panel within a Conduit Box

The conduit box must be mounted prior to continuing this section. Refer to the procedures in the *Pre-Wall Installation of the Conduit Box* section on page 28 for detailed pre-wall installation instructions. *Verify that all necessary cables have been threaded through the knockouts on the left of the conduit box and the connections have been tested prior to installation of the NXD-700Vi.*

1. Remove the Faceplate/bezel (**A** in FIG. 12) from the main NXD unit (**B** in FIG. 12) by gripping the faceplate and pulling with gentle outward force.

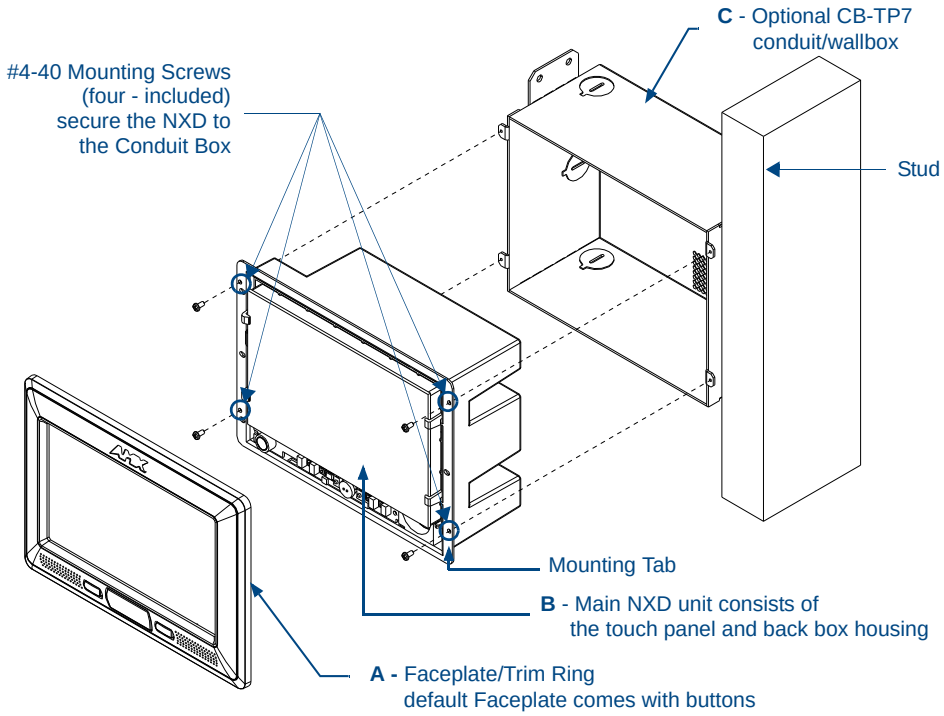


FIG. 12 NXD-700Vi panel installation into a CB-TP7 (pre-wall construction)

2. Verify the incoming power, RJ-45 audio/video, Ethernet, and USB cables have been properly threaded through the wiring knockouts on the left of the conduit box. *Leave enough slack in the wiring to accommodate any re-positioning of the panel.*
3. Connect all data and power wiring connectors to their corresponding locations along the side of the (un-powered) NXD touch panel.
   - Verify that the terminal end of the power cable is not connected to a power source before plugging in the 2-pin power connector.
   - The USB connectors can be from either a USB extension cable, or a wireless USB RF transmitter.
4. Test the incoming wiring by connecting the panel connections to their terminal locations and applying power. Verify that the panel is receiving power and functioning properly to prevent repetition of the installation.

5. Disconnect the terminal end of the power cable from the connected power supply.

NOTE

Don't disconnect the connectors from the touch panel. The unit must be installed with the attached connectors before being inserted into the conduit box.

6. Carefully slide the main NXD-700Vi unit (**B** in FIG. 12) into the conduit box, so that all Mounting Tabs lie flush against the conduit box (**C** in FIG. 12).
7. Insert and secure four #4-40 Mounting Screws (included) into their corresponding holes located along the sides of the NXD.
8. Place the Faceplate/Trim Ring assembly (**A** in FIG. 12) back onto the main NXD unit (**B** in FIG. 12). *Make sure to align the Microphone, Light, and PIR Motion sensor locations to their respective openings on the front faceplate/bezel.*
9. Reconnect the terminal RJ-45, Ethernet, USB, and any optional audio/video wiring to their respective locations (*outside the conduit box*) on either the NXA-AVB/ETHERNET Breakout Box, Ethernet port, or NetLinx Master.
10. Reconnect the terminal power connector on the 12 VDC-compliant power supply and apply power.

Installing the NXD into drywall using Expansion Clips

Expansion clips are mounted through the three oval holes located along the rim of the NXD-700Vi. As the screw is tightened, the clip bends toward the insertion hole and into the wall. This bending creates a "grip" on the wall by either pressing onto the wall or by securing the drywall between the housing and the drywall clip.

The most important thing to remember when mounting the NXD is that the outer frame (Mounting Tabs) must be installed flush against the mounting surface.

- Refer to **SP-2258-01** for detailed installation dimensions (reproduced in FIG. 13).
- It is recommended that you cutout the surface slightly smaller than what is outlined in the installation drawings so that you can make any necessary cutout adjustments.

1. Prepare the area by removing any screws or nails from the drywall before beginning the cutout process.
2. Cut out the surface for the NXD Wall Mount unit using the dimensions shown in FIG. 13. Be sure to cut out the three notches along the sides to accommodate the three corresponding drywall expansion clips (included).

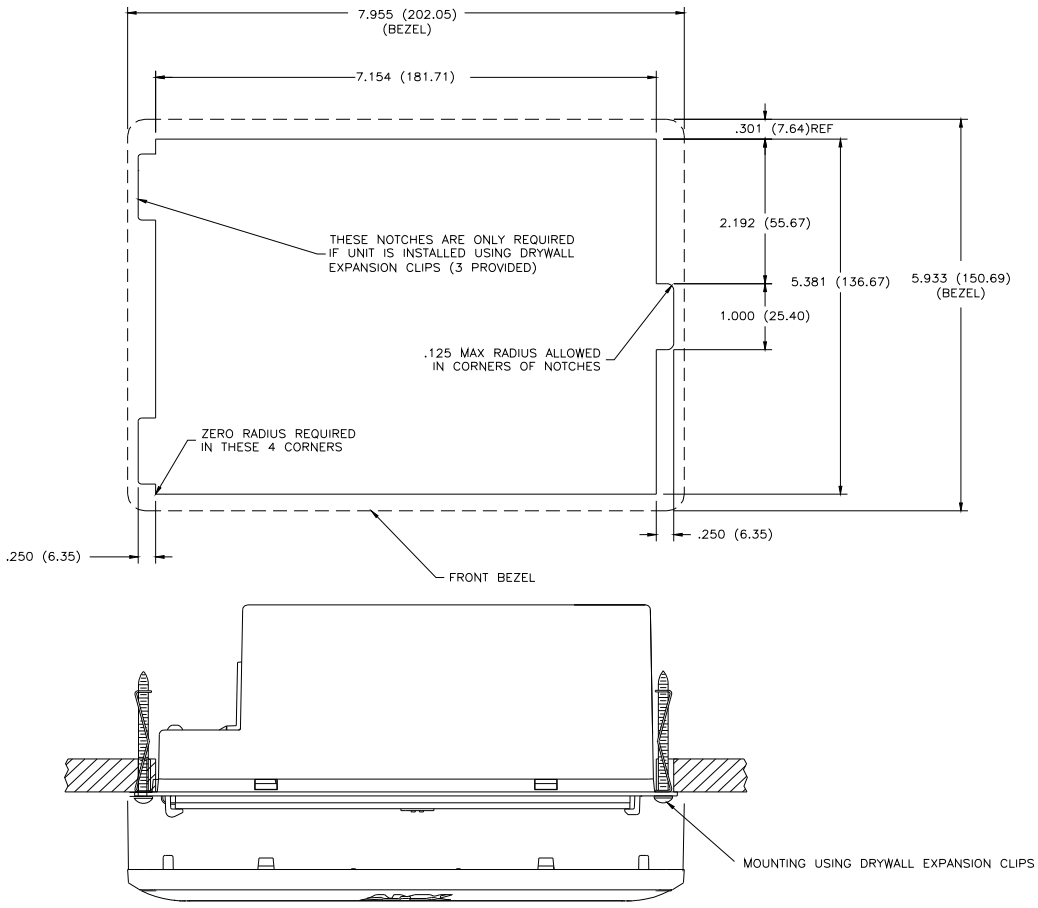


FIG. 13 NXD-700Vi Wall Mount panel dimensions using expansion clips

3. Remove the Faceplate/bezel (**A** in FIG. 14) from the main NXD unit (**B** in FIG. 14) by gripping the faceplate and pulling with gentle outward force.
4. Thread the incoming power, RJ-45, Ethernet, USB, and any optional audio/video wiring (from their terminal locations) through the surface opening. *Leave enough slack in the wiring to accommodate any re-positioning of the panel.*
5. Connect all data and power wiring connectors to their corresponding locations along the left side of the (un-powered) NXD touch panel.
   - Verify that the terminal end of the power cable is not connected to a power source before plugging in the 2-pin power connector.
   - The USB connectors can be from a either a USB extension cable, or a wireless USB RF transmitter.
6. Test the incoming wiring by attaching the panel connections to their terminal locations and applying power. Verify the panel is receiving power and functioning properly to prevent repetition of the installation.
7. Disconnect the terminal end of the power cable from the connected power supply.

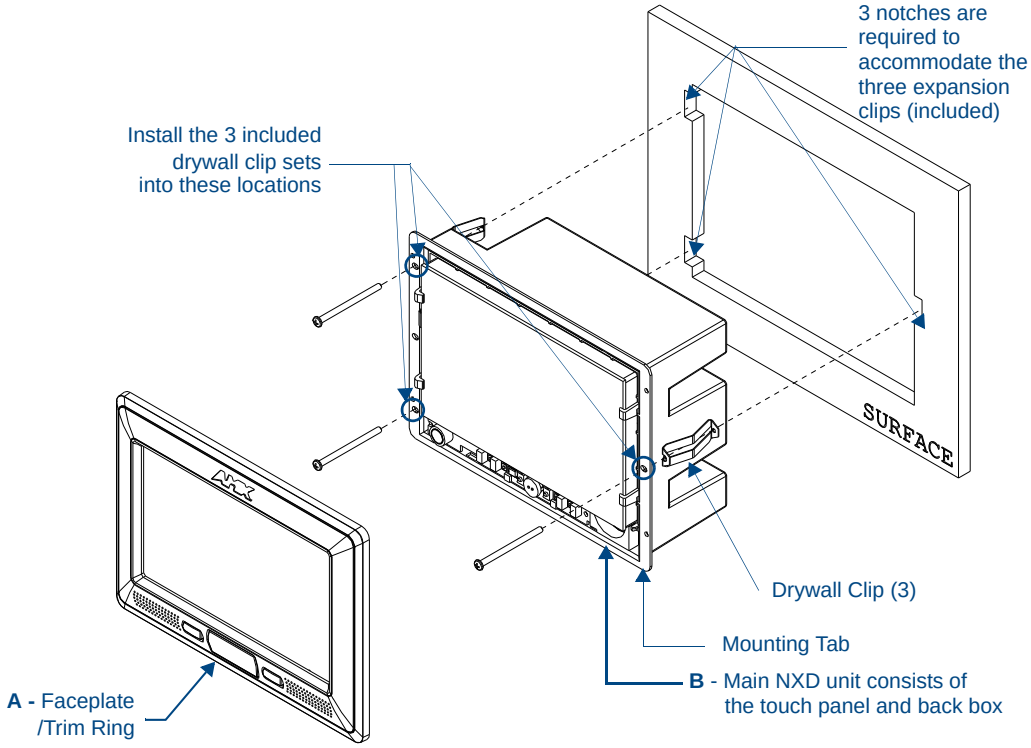


FIG. 14 Wall Mount panel (NXD) installation configuration for drywall surfaces

NOTE

Don't disconnect the connectors from the touch panel. The unit must be installed with the attached connectors before being inserted into the drywall.

8. Install the three sets of drywall screws and expansion clips into the three oval notch locations along both sides of the main unit (**B** in FIG. 14).
9. Carefully insert the main unit (with expansion clips) into the cutout until the Mounting Tabs on the NXD unit lie flush against the wall.

WARNING

The drywall clip set must be re-ordered from AMX if the drywall clip is bent accidentally during an installation or removed during a re-installation.

10. Tighten all three drywall clip sets (screws and clips) until the entire Mounting Tab is securely fastened and flush against the wall.
11. Place the Faceplate/Trim Ring assembly (**A** in FIG. 14) back onto the main NXD unit (**B** in FIG. 14). *Make sure to align the Microphone, Light, and PIR Motion sensor locations to their respective openings on the front faceplate/bezel.*
12. Reconnect the terminal RJ-45, Ethernet, USB, and any optional audio/video wiring to their respective locations on either the NXA-AVB/ETHERNET Breakout Box, Ethernet port, or NetLinx Master.
13. Reconnect the terminal power connector on the 12 VDC-compliant power supply and apply power.

Installing the NXD into a Flat Surface using #4 screws

Mounting screws (#4-40, included) are secured through two sets of circular holes located at the left and right sides of the NXD-700Vi. **The most important thing to remember when mounting the NXD Wall Mount is that the outer frame (Mounting Tabs) must be installed flush against the mounting surface.**

- Refer to **SP-2258-01** for detailed installation dimensions (reproduced in FIG. 15).
- It is recommended that you cutout the surface slightly smaller than what is outlined in the installation drawings so that you can make any necessary cutout adjustments.

1. Prepare the area by removing any screws or nails from the surface before beginning the cutout process.
2. Cut out the surface for the NXD Wall Mount unit using the dimensions shown in FIG. 15.

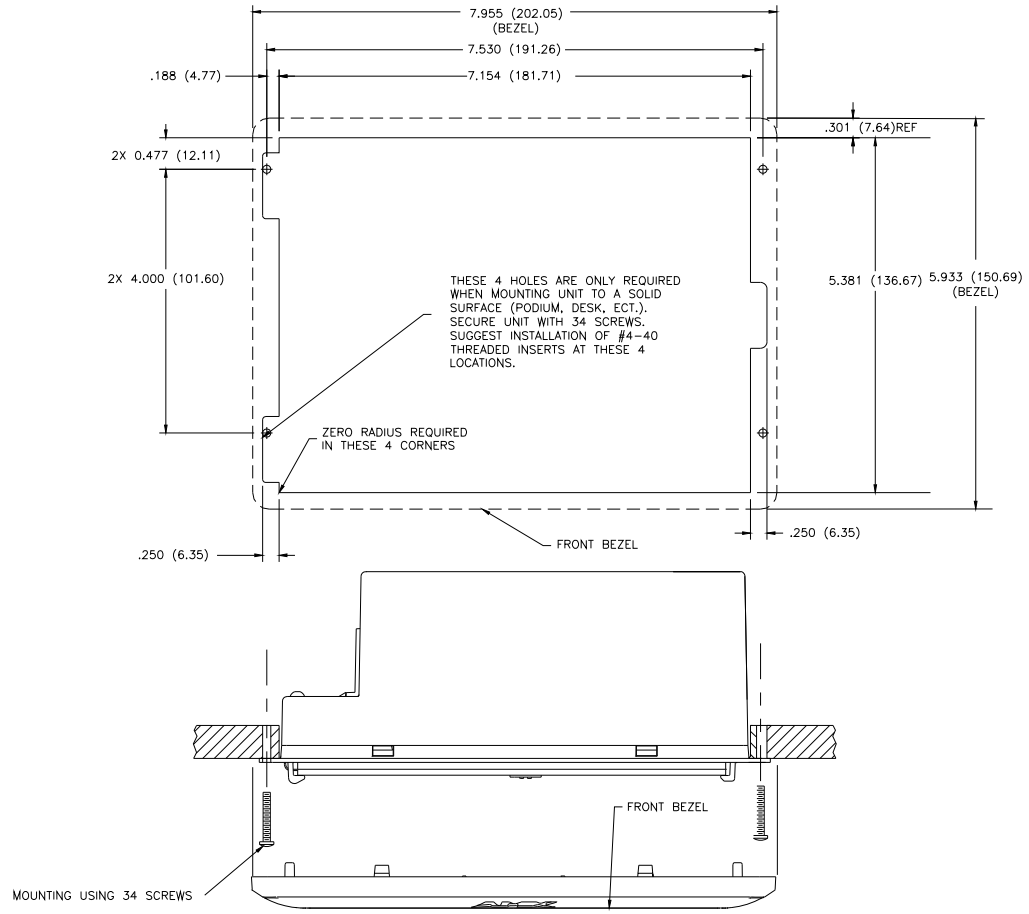


FIG. 15 NXD-700Vi Wall Mount panel dimensions using #4-40 mounting screws

3. Remove the Faceplate/bezel (**A** in FIG. 16) from the main NXD unit (**B** in FIG. 16) by gripping the faceplate and pulling with gentle outward force.
4. Thread the incoming power, RJ-45, Ethernet, USB, and any optional audio/video wiring (from their terminal sources) through the surface opening. *Leave enough slack in the wiring to accommodate any re-positioning of the panel.*
5. Connect all data and power wiring connectors to their corresponding locations along the left side of the (un-powered) NXD touch panel.
   - Verify that the terminal end of the power cable is not connected to a power source before plugging in the 2-pin power connector.
   - The USB connectors can be from a either a USB extension cable, or a wireless USB RF transmitter.
6. Test the incoming wiring by connecting the panel connections to their terminal locations and applying power. Verify that the panel is receiving power and functioning properly before finalizing the installation.

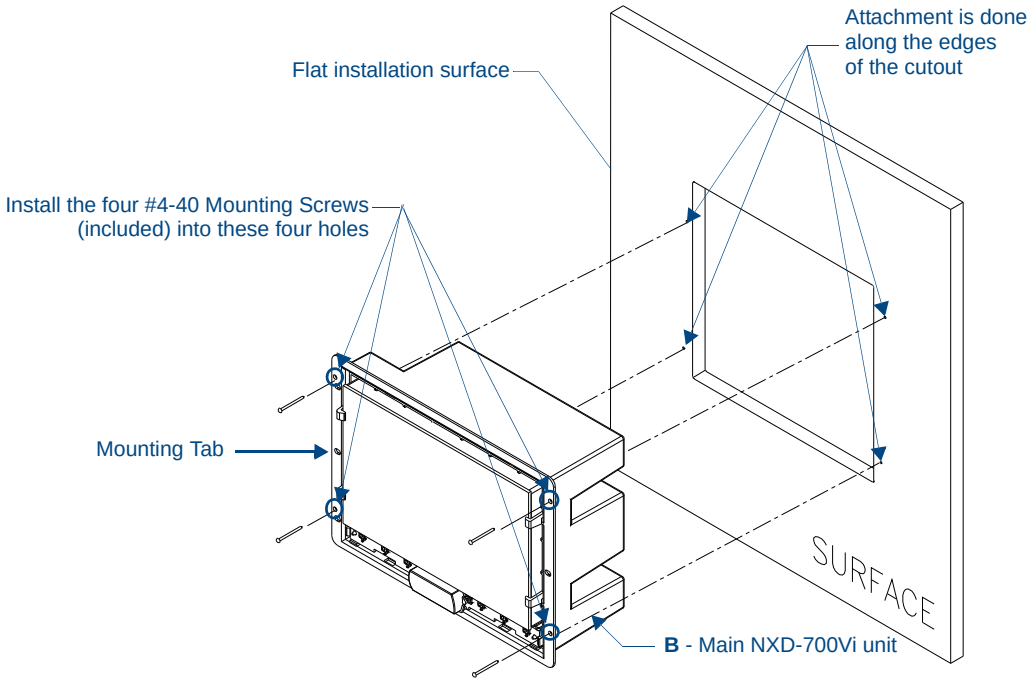


FIG. 16 Wall Mount panel installation configuration for flat surfaces

7. Disconnect the terminal end of the power cable from the power supply.

NOTE

Don't disconnect the connectors from the touch panel. The unit must be installed with the necessary connectors before being inserted into the solid surface.

8. Carefully slide the main unit into the cutout until the Mounting Tabs of the NXD-700Vi unit lie flush against the wall.
9. Insert and secure four #4-40 Mounting Screws (included) into their corresponding holes located along the sides of the NXD-700Vi (using a grounded Phillips-head screwdriver) until the unit is secure and flush against the wall (FIG. 16).
10. Place the Faceplate/Trim Ring assembly (**A** in FIG. 16) back onto the main unit (**B** in FIG. 16). *Make sure to align the Microphone, Light, and PIR Motion sensor locations to their respective openings on the front bezel/faceplate.*
11. Reconnect the terminal RJ-45, Ethernet, USB, and any optional audio/video wiring to their respective locations on either the NXA-AVB/ETHERNET Breakout Box, Ethernet port, or NetLinx Master.
12. Reconnect the terminal power connector on the 12 VDC-compliant power supply and apply power.

Installing an NXD-700Vi into an (optional) Rack Mount Kit (NXA-RK7)

The NXA-RK7 is a 19" (48.3 cm) wide metal rack-mount (with black matte finish) measuring 4 rack units high.

1. Remove the Faceplate/Trim Ring assembly from the main NXD-700Vi unit.
2. Thread the incoming power, RJ-45 audio/video, Ethernet, and USB wiring (from their terminal sources) through the surface opening, leaving enough slack in the wiring to accommodate any re-positioning of the panel.
3. Connect all data and power wiring connectors to their corresponding locations along the left side of the (un-powered) NXD touch panel.
   - Verify that the terminal end of the power cable is not connected to the a power supply before plugging in the 2-pin power connector.
   - The USB connectors can be from a either a USB extension cable, or a wireless USB RF transmitter.

4. Test the incoming wiring by connecting the panel connections to their terminal locations and applying power. Verify that the panel is receiving power and functioning properly to prevent repetition of the installation.
5. Disconnect the terminal end of the power cable from the connected power supply.

NOTE

Don't disconnect the connectors from the touch panel. The unit must be installed with the necessary connectors before being inserted into the equipment rack.

6. Carefully insert the NXD-700Vi panel into the NXA-RK7.
7. Secure the panel to the NXA-RK7 mount by first inserting and then tightening the four #4-40 screws.
8. Insert the NXA-RK7 (with connected NXD unit) into the equipment rack, making sure to align the screw holes along the sides on the NXA-RK7 with the holes in the equipment rack.
9. Use a grounded Phillips-head screwdriver to secure the NXA-RK7 to the equipment rack using #10-32 screws (included).
10. Place the Faceplate/Trim Ring assembly back onto the main NXD unit. *Make sure to align the Microphone, Light, and PIR Motion sensor locations to their respective openings on the front faceplate/ bezel.*
11. Reconnect the terminal RJ-45 audio/video, Ethernet, and USB wiring to their respective terminal locations on either the NXA-AVB/ETHERNET Breakout Box, Ethernet port, or NetLinx Master.
12. Reconnect the terminal power connector on the 12 VDC-compliant power supply and apply power.

Wiring Guidelines for the NXD-700Vi Panels

NXD-700Vi panels use a 12 VDC-compliant power supply to provide power to the panel via the 2-pin 3.5 mm mini-Phoenix PWR connector. Use the previously provided power requirement information to determine the power draw.

The incoming PWR and GND wires from the power supply must be connected to the corresponding locations within the PWR connector.

WARNING

These units should only have one source of incoming power. Using more than one source of power to the touch panel can result in damage to the internal components and a possible burn out.
*Apply power to the panels **only after** installation is complete.*

Preparing Captive Wires

You will need a wire stripper and flat-blade screwdriver to prepare and connect the captive wires.

WARNING

Never pre-tin wires for compression-type connections.

1. Strip 0.25 inch (6.35 mm) of insulation off all wires.
2. Insert each wire into the appropriate opening on the connector (according to the wiring diagrams and connector types described in this section).
3. Tighten the screws to secure the wire in the connector. Do not tighten the screws excessively; doing so may strip the threads and damage the connector.

Wiring a Power Connection

To use the 2-pin 3.5 mm mini-Phoenix connector with a 12 VDC-compliant power supply, the incoming PWR and GND wires from the external source must be connected to their corresponding locations on the connector (FIG. 17).

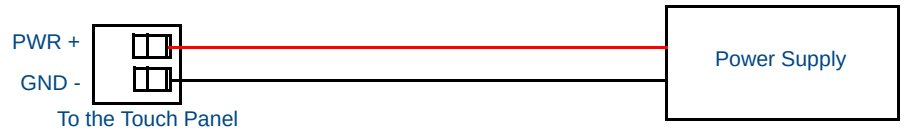


FIG. 17 NetLinx power connector wiring diagram

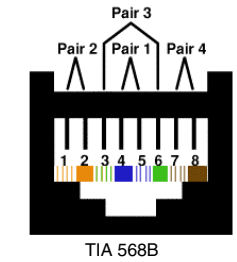
1. Insert the PWR and GND wires on the terminal end of the 2-pin 3.5 mm mini-Phoenix cable. ***Match the wiring locations of the +/- on both the power supply and the terminal connector.***
2. Tighten the clamp to secure the two wires. *Do not tighten the screws excessively; doing so may strip the threads and damage the connector.*
3. Verify the connection of the 2-pin 3.5 mm mini-Phoenix to the external 12 VDC-compliant power supply.

Audio/Video Port: Connections and Wiring

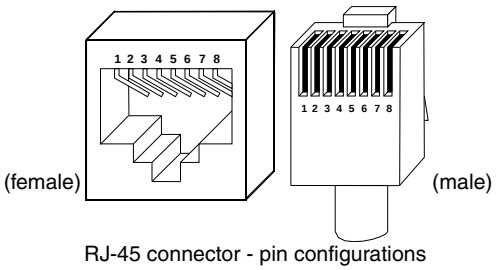
The following table shows the signal and pinout/pairing information used on the RJ-45 Audio and Video connections.

Audio/Video RJ-45 Pinout Information

Pin	Wire Color	Function	Polarity
1	Orange/White	Right Audio In	+
2	Orange	Right Audio In	-
3	Green/White	Video In	-
4	Blue	Mic Out	-
5	White/Blue	Mic Out	+
6	Green	Video In	+
7	White/Brown	Left Audio In	+
8	Brown	Left Audio In	-



TIA 568B



RJ-45 connector - pin configurations

Ethernet/RJ-45 Port: Connections and Wiring

FIG. 18 describes the blink activity for the Ethernet 10/100 Base-T RJ-45 connector and cable. The Ethernet cable is connected to the rear of Table Top and side of the Wall Mount panels.

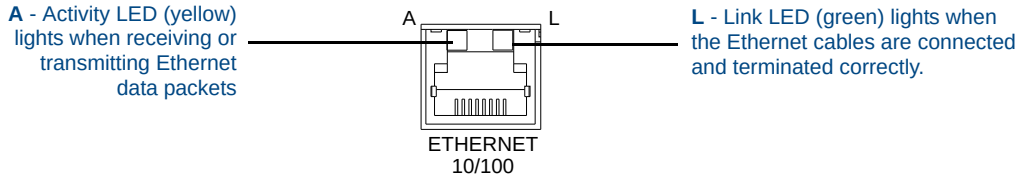


FIG. 18 Ethernet connector (showing communication and connection LEDs)

The following table lists the pinouts, signals, and pairing associated with the Ethernet connector.

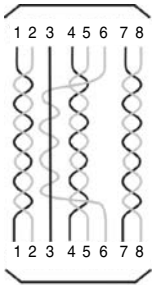
Ethernet RJ-45 Pinouts and Signals					
Pin	**Signals**	**Connections**	**Pairing**	**Color**	
1	TX +	1 -------- 1	1 -------- 2	Orange-White	
2	TX -	2 -------- 2		Orange	
3	RX +	3 -------- 3	3 -------- 6	Green-White	
4	no connection	4 -------- 4		Blue	
5	no connection	5 -------- 5	4 -------- 5	Blue-White	
6	RX -	6 -------- 6		Green	
7	no connection	7 -------- 7	7 -------- 8	Brown-White	
8	no connection	8 -------- 8		Brown	

FIG. 19 diagrams the RJ-45 pinouts and signals for the Ethernet RJ-45 connector and cable.

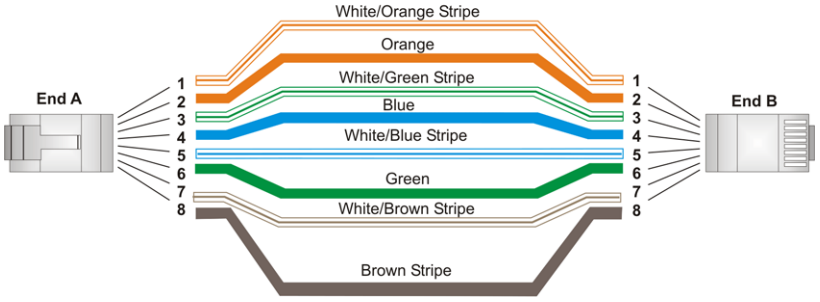


FIG. 19 RJ-45 wiring diagram

USB Port: Connecting and Using Input Devices

The NXD-700Vi panel can have up to two USB-capable input devices connected for use on its different firmware and TPD4 panel pages. These input devices can consist of a keyboard or mouse.

NOTE

USB-connected input devices are not detected and recognized by the panel until power is cycled to the unit.
A mini-USB connection is only detected after it is installed onto an active panel. Connection to a previously powered panel, allows the PC to detect the panel and assign an appropriate USB driver.

1. Insert the input device USB connectors into the appropriate USB connector on the panel.
2. Press the on-screen **Reboot** button from the Protected Setup page to save any changes and restart the panel.
3. After the panel splash-screen disappears:

- If a USB mouse has been connected, a mouse cursor appears on the panel screen and its location corresponds to the mouse cursor position sent by the external USB mouse.
- If a USB keyboard has been connected, only on-screen keyboards and keypads will reflect any external keystrokes sent from the external USB keyboard.

Panel Calibration

Overview

This section outlines the steps for calibrating the touch panel. *It is recommended that you calibrate the panel before its initial use and after completing a firmware download.*

Modero panels are factory setup with specific demo touch panel pages. The first splash screen that appears indicates the panel is receiving power, beginning to load firmware, and preparing to display the default touch panel pages. When the panel is ready, the AMX Splash Screen is replaced by the Initial Panel Page (FIG. 20).

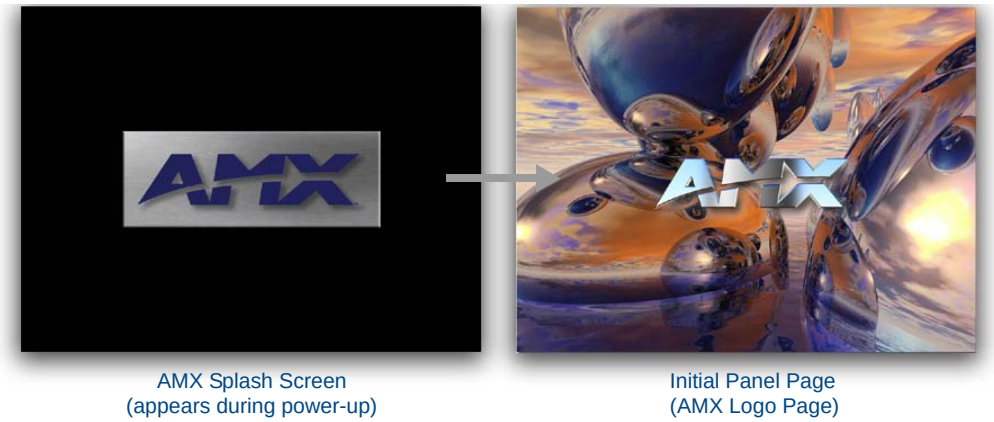


FIG. 20 AMX splash screen and initial Panel Page

Calibrating the Modero Panel

1. Press and hold the grey Front Setup Access button (FIG. 21) for **6 seconds** to pass-over the Setup page and access the Calibration setup page (FIG. 22).

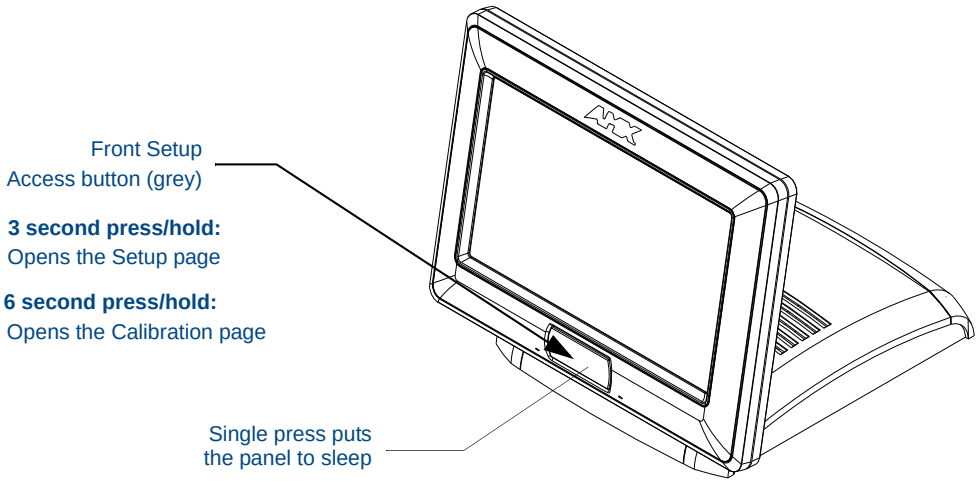


FIG. 21 Location of Front Setup Access button

2. Press the crosshairs (on the Calibration page) to set the calibration points on the LCD (FIG. 22).
3. After the "***Calibration Successful.***." message appears, press anywhere on the screen to continue and return to the Setup page.

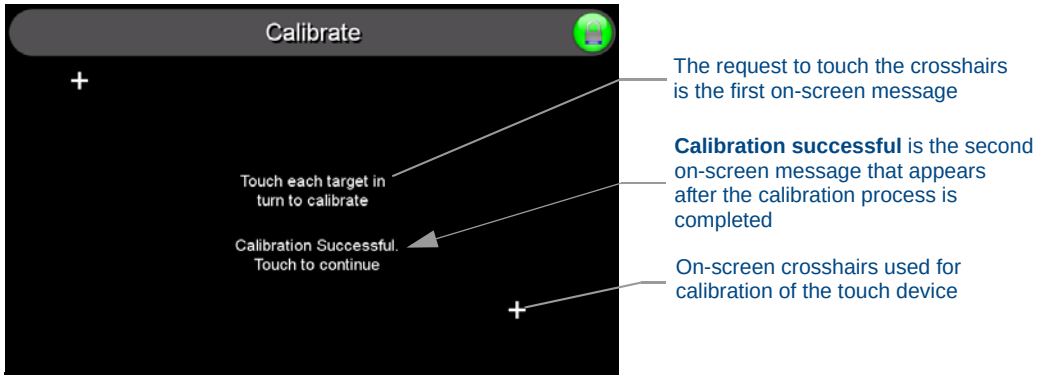


FIG. 22 Touch Panel Calibration Screens

NOTE

If the calibration was improperly set and you cannot return to the Calibration page (through the panel's firmware); *you can then access this firmware page via G4 WebControl where you can navigate to the Protected Setup page and press the Calibrate button through your VNC window.*
This action causes the panel to go to the Calibration page seen above, where you can physically recalibrate the actual touch panel again using the above procedures.

Testing your Calibration

1. Press and hold down the on-screen **Calibration** button for 6 seconds to enter the Calibration Test page (FIG. 23).

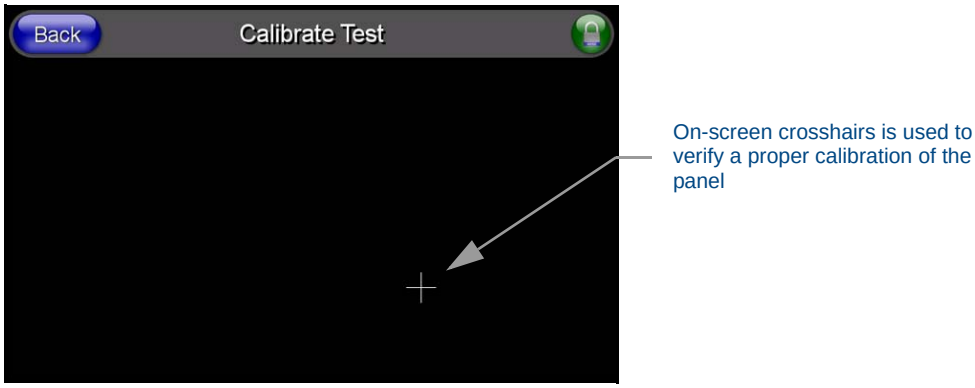


FIG. 23 Calibration Test page

2. Press anywhere on this page to confirm the on-screen crosshairs match your touch points.
3. If the crosshairs do not appear directly below your LCD touch points, press the **Back** button and recalibrate the panel using the above steps.

Peel the protective plastic film from the LCD.

NOTE

If the protective plastic film on the LCD is not removed, the panel may not respond properly to touch points on the LCD nor allow proper screen calibration.

4. Exit this Calibration Test page by pressing the **Back** button to return to the Protected Setup page.

If Calibration Is Not Working

Cycling power to the panel should provide a baseline calibration for the particular touch panel. Re-calibrate the panel.

Configuring Communication

Overview

Communication between the Modero panel and the Master is done using either **USB** or **ETHERNET** (**DHCP or Static IP**). Ethernet communication can be achieved through either a direct connection (Ethernet) or through the use of the optional NXA-WC802.11GCF wireless CF card.

WARNING

Before commencing, verify you are using the latest NetLinx Master and Modero panel firmware. Verify you are using the latest versions of AMX's NetLinx Studio and TPDesign4 programs.

NOTE

USB input devices must be plugged into the rear or side USB connectors before the G4 panel is powered-up. The panel will not detect a USB connection of this type until after the unit cycles power.

Modero Setup and System Settings

AMX Modero panels feature on-board Setup pages. Use the options in the Setup pages to access panel information and make various configuration changes.

Accessing the Setup and Protected Setup Pages

1. Press the grey Front Setup Access button for **3 seconds** to open the Setup page (FIG. 24).

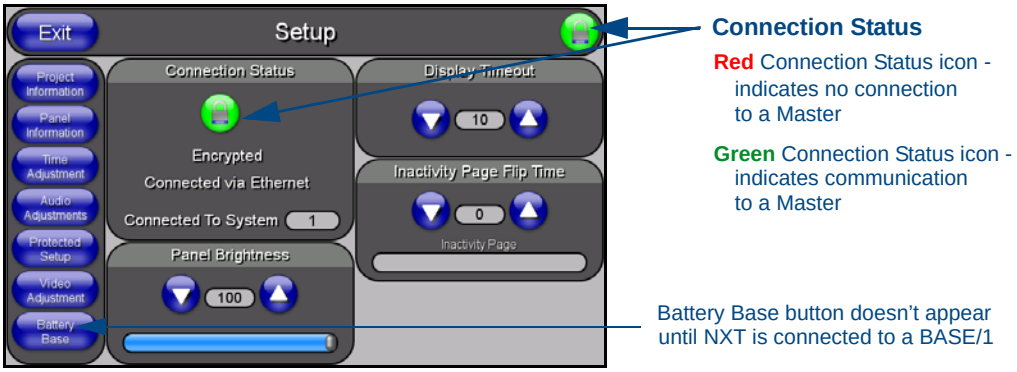


FIG. 24 Setup page

2. Press the Protected Setup button. This invokes a keypad for entry of the password to allow access to the Protected Setup page. Enter **1988** (the default password), and press **Done** to proceed.

NOTE

Clearing Password #5, from the initial Password Setup page, removes the need for you to enter the default password before accessing the Protected Setup page.

Setting the Panel's Device Number

In the *Protected Setup* page:

1. Press the *Device Number* field to open the Device Number keypad (FIG. 25).

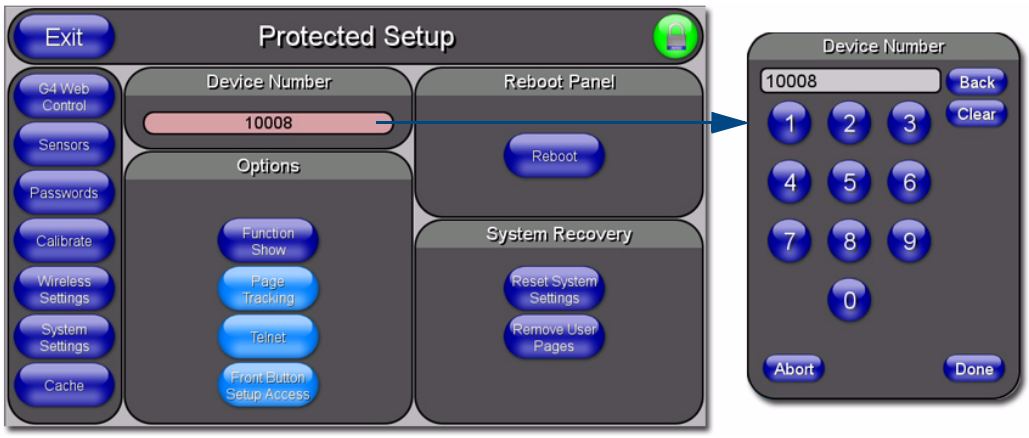


FIG. 25 Protected Setup page

   Enter a unique Device Number assignment for the panel**,** and press **Done** to return to the *Protected Setup* page. The Device Number range is 1 - 32000, the default is **10001**.

2. Press **Reboot** to reboot the panel, and apply the new Device Number.

Wireless Settings Page - Wireless Access Overview

Hot Swapping

Hot swapping is not an issue on these panels as the card is installed within the unit and cannot be removed without first removing the housing.

In the case of DHCP, there must be a DHCP server accessible before the fields are populated.

NOTE

If the SSID (Network Name) and WEP fields have not previously been configured, the Wireless Settings page will not work until the panel is rebooted.

Before selecting **Ethernet** as the Master Connection Type you must setup the parameters of the wireless card. **The Wireless Access Point communication parameters must match those of the pre-installed wireless CF card inside the panel.**

The panels allow users to connect to a wireless network through their use of the pre-installed AMX 802.11g wireless interface card to communicate with a Wireless Access Point (WAP) such as the NXA-WAP200G). The WAP communication parameters must match those of the pre-installed wireless interface card installed within the panel. This internal card transmits data wirelessly using the 802.11x signals at 2.4 GHz. For a more detailed explanation of the new security and encryption technology, refer to the section of the document entitled: *Appendix B - Wireless Technology* section on page 197.

For more information on utilizing the AMX Certificate Upload Utility in conjunction with the EAP security, refer to the section of the document entitled: *Appendix B - Wireless Technology* section on page 197.

Configuring a Wireless Network Access

When working with a wireless card, the first step is to configure wireless communication parameters within the Wireless Settings page. This page only configures the card to communicate to a target WAP (such as the NXA-WAP200G), **it is still necessary to tell the panel which Master it should be communicating with**. This "pointing to a Master" is done via the System Settings page where you configure the IP Address, System Number and Username/Password information assigned to the target Master.

Step 1: Configure the Panel's Wireless IP Settings

The first step to successfully setting up your internal wireless card is to configure the IP Settings section on the Wireless Settings page. The section configures the communication parameters from the panel to the web.

Wireless communication using a DHCP Address

In the *Protected Setup* page:

1. Select **Wireless Settings**. Wireless communication is set within the IP Settings section of this page (FIG. 26).
2. Toggle the *DHCP/Static* field (from the IP Settings section) until the choice cycles to *DHCP*. This action causes all fields in the IP Settings section (other than Host Name) to be greyed-out.

Do not alter any of these remaining greyed-out fields in the IP Settings section. Once the panel is rebooted, these values are obtained by the unit and displayed in the *DNS* fields after power-up.

NOTE

DHCP will register the unique MAC Address (factory assigned) on the panel and once the communication setup process is complete, assign IP Address, Subnet Mask, and Gateway values from the DHCP Server.

3. Press the optional *Host Name* field to open a Keyboard and enter the Host Name information.

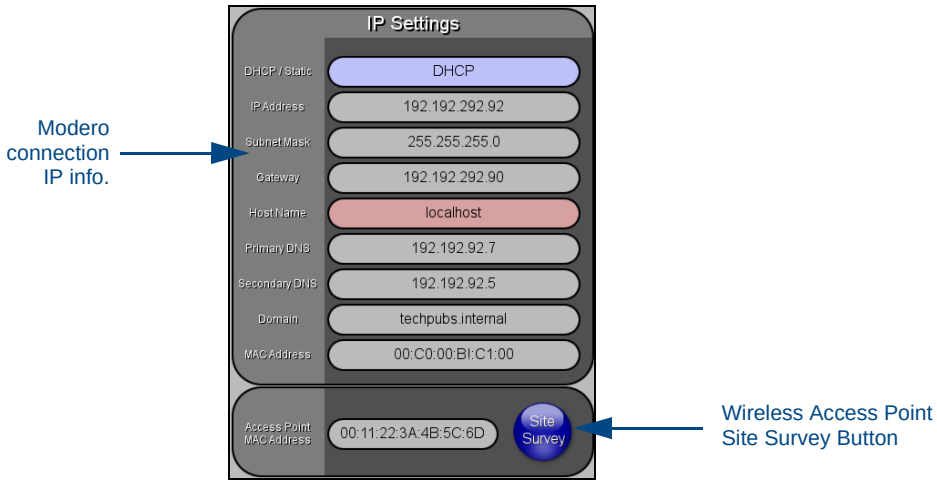


FIG. 26 Wireless Settings page (IP Settings section)

4. Press **Done** after you are finished assigning the alpha-numeric string of the host name.
5. Do not alter any of these remaining greyed-out fields in the IP Settings section. Once the panel is rebooted, these values are obtained by the unit and displayed in the *DNS* fields after power-up.

NOTE

This information can be found in either the Workspace - System name > Define Device section of your code (that defines the properties for your panel), or in the Device Addressing/Network Addresses section of the Tools > NetLinx Diagnostics dialog.

6. Setup the security and communication parameters between the wireless card and the target WAP by configuring the Wireless Settings section on this page. Refer to *Step 2: Configure the Card's Wireless*

Security Settings section on page 46 for detailed procedures to setup either a secure or unsecure connection.

Wireless communication using a Static IP Address

In the *Protected Setup* page:

1. Press the **Wireless Settings** button (located on the lower-left) to open the Wireless Settings page. Wireless communication is set within the IP Settings section of this page (FIG. 26).

Check with your System Administrator for a pre-reserved Static IP Address assigned to the panel. This address must be obtained before Static assignment of the panel continues.

2. Toggle the *DHCP/Static* field (***from the IP Settings section***) until the choice cycles to **Static**. *The IP Address, Subnet Mask, and Gateway fields then become user-editable (red).*
3. Press the *IP Address* field to open a Keyboard and enter the Static IP Address (*provided by your System Administrator*).
4. Press **Done** after you are finished entering the IP information.
5. Repeat the same process for the *Subnet Mask* and *Gateway* fields.
6. Press the optional *Host Name* field to open the Keyboard and enter the Host Name information.
7. Press **Done** after you are finished assigning the alpha-numeric string of the host name.
8. Press the Primary DNS field to open a Keyboard, enter the Primary DNS Address (provided by your System Administrator) and press **Done** when compete. Repeat this process for the Secondary DNS field.
9. Press the Domain field to open a Keyboard, enter the resolvable domain Address (this is provided by your System Administrator and equates to a unique Internet name for the panel), and press **Done** when complete.
10. Setup the security and communication parameters between the wireless card and the target WAP by configuring the Wireless Settings section on this page. Refer to the following section for detailed procedures to setup either a secure or unsecure connection.

Using the Site Survey tool

This tool allows a user to "sniff-out" all transmitting Wireless Access Points within the detection range of the internal NXA-WC80211GCF. Once pressed, the panel displays the Site Survey page which contains categories such as:

- **Network Name** (SSID) - Wireless Access Point names
- **Channel** (RF) - Channel currently being used by the WAP (*Wireless Access Point*)
- **Security Type** (if detectable - such as **WEP**, **OPEN** and **UNKNOWN**) - security protocol enabled on the WAP
- **Signal Strength** - None, Poor, Fair, Good, Very Good, and Excellent
- **MAC Address** - Unique identification of the transmitting Access Point

In the *Protected Setup* page:

1. Press the **Wireless Settings** button (located on the lower-left) to open the Wireless Settings page.
2. Navigate to the Access Point MAC Address section of this page and press the on-screen **Site Survey** button. This action launches the Site Survey page which displays a listing of all detected WAPs in the communication range of the internal card.
   - The card scans its environment every four seconds and adds any new WAPs found to the list. Every scan cycle updates the signal strength field.
   - Access points are tracked by MAC Address.
     - If the WAP's SSID is set as a blank, then **N/A** is displayed within the *SSID* field.
     - If the WAP's SSID is hidden (*not broadcast*) it will not show up on the site survey screen but it can still be configured via the *SSID* field on the specified security mode screen.

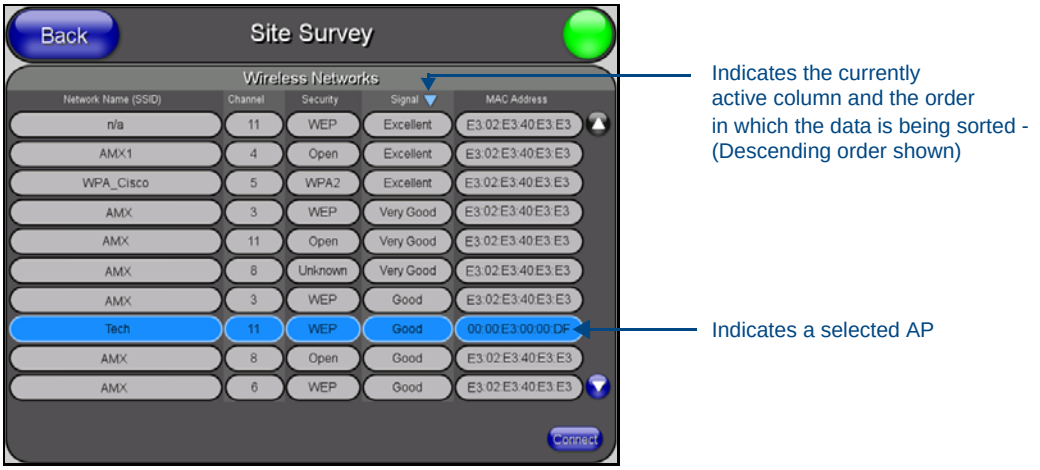


FIG. 27 Site Survey page

- If a WAP is displayed in the list is not detected for 10 scans in a row it is then removed from the screen. In this way, a user can walk around a building and see access points come and go as they move in and out of range.

3. Sort the information provided on this page by pressing on a column name and toggling the direction of the adjacent arrow.
   - **Up arrow** - indicates that the information is being sorted in a Ascending order.
     - **SSID** (A to Z), **Channel** (1 to 14), **Security** (Unknown to WEP), **Signal** (None to Excellent). The firmware considers the following to be the security order from least secure to most secure: Open, WEP, WPA, WPA2, and Unknown.
   - **Down arrow** - indicates that the information is being sorted in a Descending order.
     - **SSID** (Z to A), **Channel** (11 to 6), **Security** (WEP to Unknown), **Signal** (Excellent to None)

NOTE

If the panel detects more than 10 WAPs, the Up/Down arrows at the far right side of the page become active (blue) and allow the user to scroll through the list of entries.

4. Select a desired Access Point by touching the corresponding row. The up arrow and down arrow will be grayed out if there are ten or less access points detected. If there are more, then they will be enabled as appropriate so that the user can scroll through the list.
5. With the desired WAP selected and highlighted, click the **Connect** button to be directed to the selected security mode's Settings page with the *SSID* field filled in. You can then either **Cancel** the operation or fill in any necessary information fields and then click **Save**.
   *If you select an Open, WEP, and WPA-PSK Access Point and then click **Connect**, you will be flipped to the corresponding Settings page. For any other security mode, if you click **Connect** you will only return to the previous page without any information being pre-filled out for you.*
   - In an Open security mode, when a target WAP is selected and the connect to, the SSID name of the selected WAP is saved for the open security mode.
   - In a Static WEP security mode, when a WEP Access Point is selected and then connected to, the user is then redirected back to the Static WEP security screen where the *SSID* field is already filled out and the user is only required to enter in the remaining WEP key settings.
   - A similar process occurs for WPA-PSK access points. For any other case, the firmware switches back to the previous page and security and connection parameters must be entered in as normal.

Step 2: Configure the Card's Wireless Security Settings

The second step to successfully setting up your wireless card is to configure the Wireless Settings section of the Wireless Settings page. This section configures both the communication and security parameters from the internal wireless card to the WAP. ***The procedures outlined within the following sections use an 802.11g card to configure a common security configuration to a target WAP.***

Refer to either the Wireless Settings Page section on page 88 *or the Appendix B - Wireless Technology* section on page 197 *for more information on the other security methods.*

Once you have set up the wireless card parameters, you must configure the communication parameters for the target Master; see *Step 3: Choose a Master Connection Mode* section on page 52.

Configuring the Modero's wireless card for unsecured access to a WAP200G

In the *Protected Setup* page:

1. Press the **Wireless Settings** button (located on the lower-left) to open the Wireless Settings page.

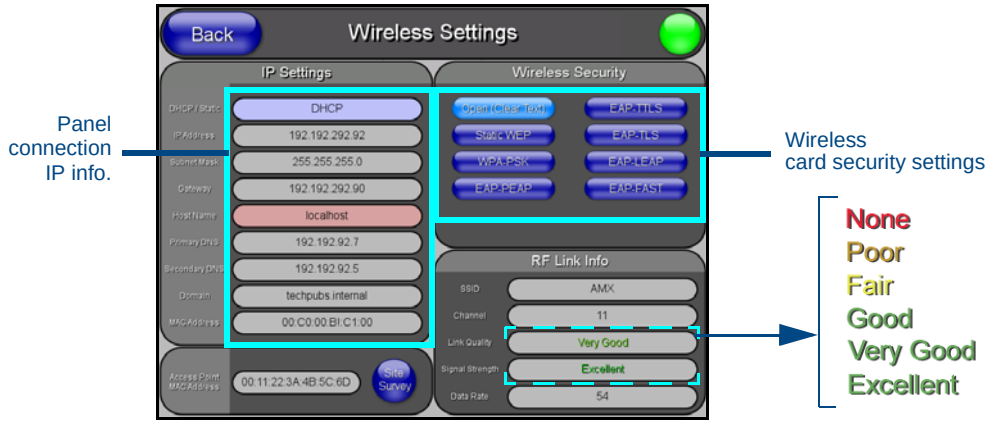


FIG. 28 Wireless Settings page (showing a sample unsecured configuration)

2. Enter the SSID information by either:
   - *Automatically* having it filled in by pressing the Site Survey button and from the Site Survey page, choosing an ***Open*** WAP from within the Site Survey page and then pressing the **Connec**t button.

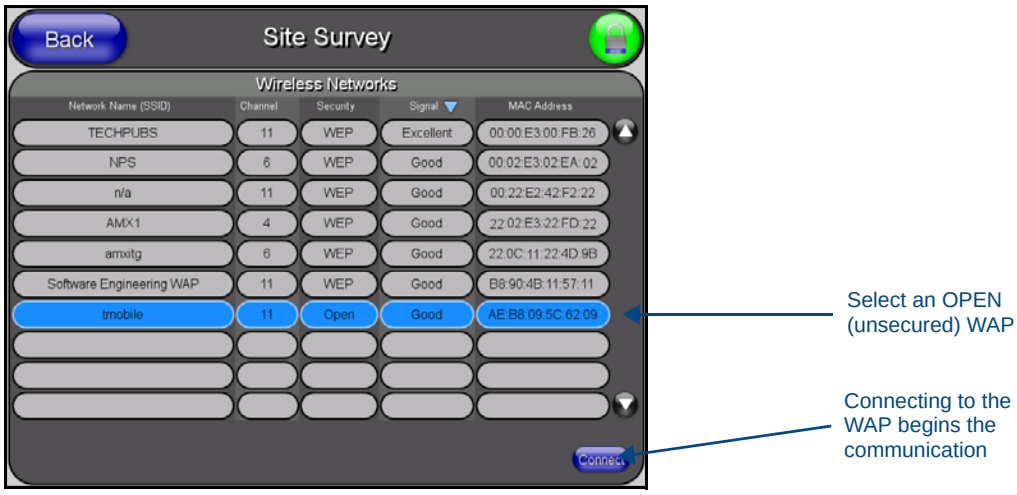


FIG. 29 Site Survey of available WAPS (Unsecured WAP shown selected)

   - *Manually* entering the SSID information into their appropriate fields by following steps 7 thru 9.

3. From within the Wireless Security section, press the **Open (Clear Text)** button to open the Open (Clear Text) Settings dialog (FIG. 30). An Open security method does not utilize any encryption methodology but does require that an SSID (alpha-numeric) be entered. Using this method causes network packets to be sent out as unencrypted text.

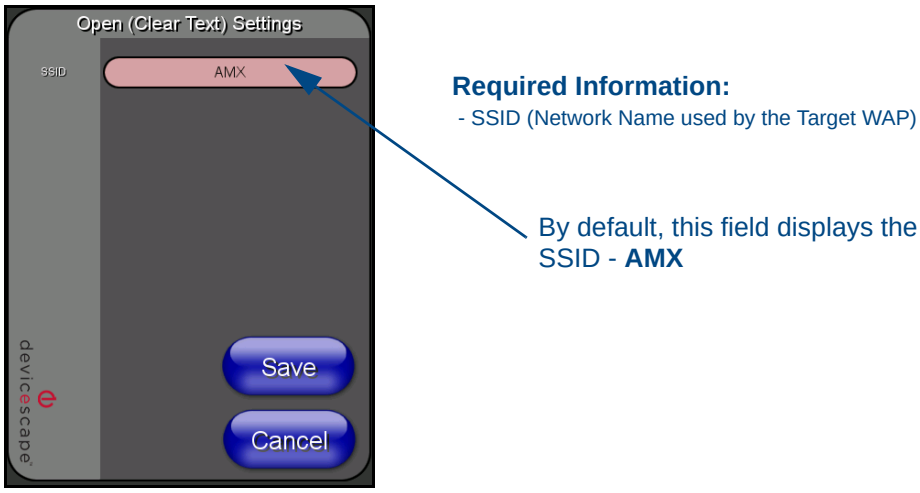


FIG. 30 Wireless Settings page - Open (Clear Text) security method

4. Press the red *SSID* field (FIG. 30) to display an on-screen *Network Name (SSID)* keyboard.
5. In this keyboard, enter the SSID name used on your target Wireless Access Point (**case sensitive**).
   - The card should be given the SSID used by the target WAP. If this field is left blank, the unit will attempt to connect to the first available WAP. By default, all WAP200Gs use **AMX** as their assigned SSID value.
   - One of the most common problems associated with connection to a WAP arise because the SSID was not entered properly. You must maintain the same case when entering the SSID information. ABC is not the same as Abc.
6. Click **Done** when you've completed typing in the information.
7. From the Open (Clear Text) Settings page (FIG. 30), press the **Save** button to incorporate your new information into the panel and begin the communication process.
8. Verify the fields in the *IP Settings* section have been properly configured. Refer to *Step 1: Configure the Panel's Wireless IP Settings* section on page 43 for detailed information.
9. Press the **Back** button to return to the Protected Setup page and press the on-screen **Reboot** button to both save any changes and restart the panel. ***Remember that you will need to navigate to the System Settings page and configure the connection to a target Master.***
10. After the panel restarts, return to the Wireless Settings page's RF Link Info section and verify the Link Quality and Signal Strength:
    - The descriptions are: **None**, **Poor**, **Fair**, **Good**, **Very Good**, and **Excellent** (FIG. 28).

NOTE

The signal strength field should provide some descriptive text regarding the strength of the connection to a Wireless Access Point. If there is no signal or no IP Address displayed; configuration of your network could be required.

Configuring the Modero's wireless card for secured access to a WAP200G

After logging into the WAP200G, the default Status page appears within the web browser. These read-only values are "pulled" from some of the other user-configurable Configuration Utility pages. By default, wireless Modero panels are configured for unsecured communication to a Wireless Access Point. To properly setup both the WAP200G and panel for secure communication, you must first prepare the Modero panel and then use the information given to fill out the fields within the WAP's browser-based Basic Wireless Configuration page.

Since the code key generator on Modero panels use the same key generation formula, all panels will generate identical keys for the same Passphrase. The generators used on WAPs will not produce the same key as the Modero generator even if you use the same Passphrase. **For this reason, we recommend FIRST creating the Current Key on the Modero and then entering that information into the appropriate NXA-WAP200G fields**.

Automatically set SSID

In the *Protected Setup* page:

1. Select **Wireless Settings**.
2. Press the **Site Survey** button.
3. Select a **WEP** secured WAP from within the Site Survey page, and press the **Connect** button.

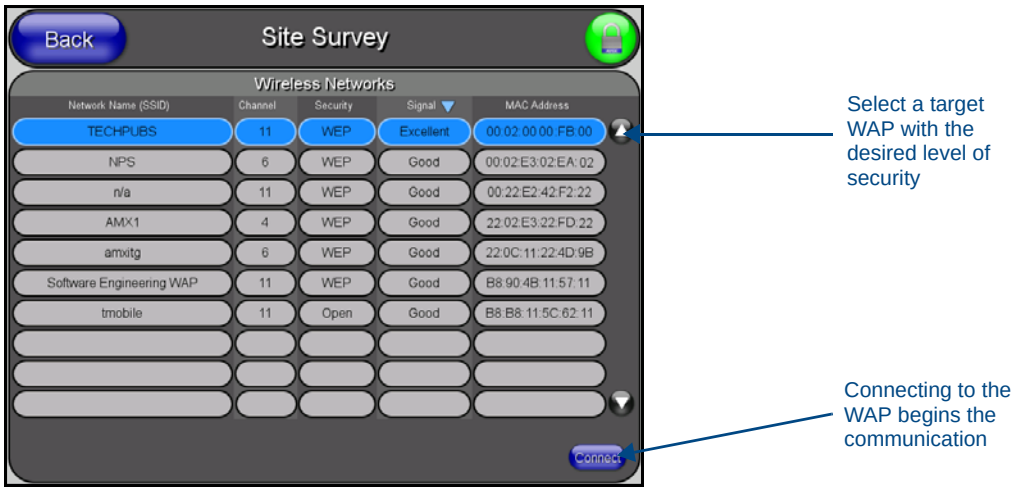


FIG. 31 Site Survey of available WAPs (Secured WAP shown selected)

4. Write down the SSID name, Current Key string value, and panel MAC Address information so you can later enter it into the appropriate WAP dialog fields in order to "sync-up" the secure connection. These values must be identically reproduced on the target WAP.

Manually set SSID

In the *Protected Setup* page:

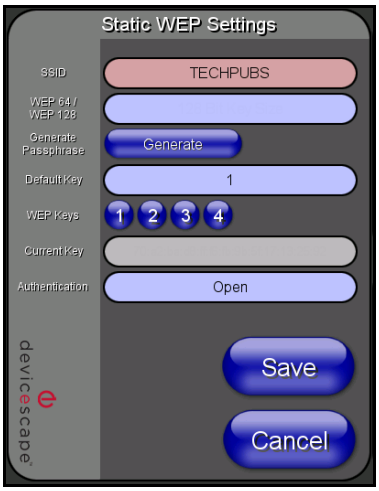
1. Select **Wireless Settings**.
2. Locate the Wireless Security section (FIG. 32).

FIG. 32 Wireless Settings page

NOTE

You must first take down the SSID name, Current Key string value, and panel MAC Address information so you can later enter it into the appropriate WAP dialog fields in order to "sync-up" the secure connection. These values must be identically reproduced on the target WAP.

3. Press the **Static WEP** button to open the Static WEP Settings dialog (FIG. 33).



Required Information:

- SSID (Network Name used by the Target WAP)
- Encryption Method
- Passphrase
- WEP Key assignment
- Authentication Method

FIG. 33 Wireless Settings page - Static WEP security method

4. Press the *SSID* field and from the *Network Name (SSID)* keyboard, enter the SSID name you are using on your target Wireless Access Point (**case sensitive**), and press **Done** when finished.
   - The card should be given the SSID used by the target WAP. If this field is left blank, the unit will attempt to connect to the first available WAP. By default, all WAP200Gs use **AMX** as their assigned SSID value.
   - One of the most common problems associated with connection to a WAP arise because the SSID was not entered properly. You must maintain the same case when entering this information. ***ABC is not the same as Abc***.
   - The alpha-numeric string is by default **AMX** but can later be changed to any 32-character entry. *This string must be duplicated within the Network Name (SSID) field on the WAP.*

- As an example, if you use **TECHPUBS** as your SSID, you must **match this word and the case** within both the *Network Name (SSID)* field on the touch panel's *Network Name SSID* field and on the WAP's *Basic Wireless Configuration* page.

5. Toggle the *Encryption* field (FIG. 33) until it reads either: **64 Bit Key Size** or **128 Bit Key Size**.
The 64/128 selection reflects the bit-level of encryption security. This WEP encryption level must match the encryption level being used on the WAP.

NOTE

WEP will not work unless the same Default Key is set on both the panel and the Wireless Access Point.
For example: if you have your Wireless Access Point set to default key 4 (which was 01:02:03:04:05), you must set the panel's key 4 to 01:02:03:04:05.

6. Toggle the *Default Key* field until the you've chosen a WEP Key value (**from 1- 4**) that matches what you'll be using on your target WAP200G. **This value MUST MATCH on both devices**.
   - **These WEP Key identifier values must match for both devices.**
7. With the proper WEP Key value displayed, press the **Generate** button to launch the WEP Passphrase keyboard.
If you are wanting to have your target WAP (other than an NXA-WAP200G) generate the Current Key - Do not press the Generate button and continue with Step 13.
   - This keyboard allows you to enter a Passphrase (such as *AMXPanel*) and then AUTOMATICALLY generate a WEP key which is compatible only among all Modero panels.

NOTE

The code key generator on Modero panels use the same key generation formula. Therefore, this same Passphrase generates identical keys when done on any Modero because they all use the same Modero-specific generator. The Passphrase generator is case sensitive.

8. Within this on-screen WEP Passphrase keyboard (FIG. 34), enter a character string or word (such as ***AMXPanel***) and press **Done** when you have finished.

FIG. 34 WEP Passphrase Keyboard

- As an example, enter the word **AMXPanel** using a 128-bit hex digit encryption. After pressing **Done**, the on-screen Current Key field displays a long string of characters (separated by colons) which represents the encryption key equivalent to the word AMXPanel.
- **This series of hex digits (26 hex digits for a 128-bit encryption key) should be entered as the *Current Key* into both the WAP and onto other communicating Modero panels by using the WEP Key dialog (FIG. 35).**

FIG. 35 WEP Key # Keyboard

9. Write down this Current Key string value for later entry into your WAP's *WEP Key* field (*typically entered without colons*) and into other communicating panel's *Current Key* field (FIG. 35).
10. **If you are entering a Current Key generated either by your target WAP or another Modero panel**, within the *WEP Keys* section, touch the **Key #** button to launch the *WEP Key #* keyboard (FIG. 35), enter the characters and press **Done** when finished.
    - This Key value corresponds to the Default WEP Key number used on the Wireless Access Point and selected in the Default Key field described in the previous step.

NOTE

If your target Wireless Access Point does not support passphrase key generation and has previously been setup with a manually entered WEP KEY, you must manually enter that same WEP key on your panel.

11. The remaining *Current Key* and *Authentication* fields are greyed-out and cannot be altered by the user.
12. Verify the fields within the IP Settings section have been properly configured. Refer to *Step 1: Configure the Panel's Wireless IP Settings* section on page 43 for detailed information.
13. Press the **Back** button to navigate to the Protected Setup page and press the on-screen **Reboot** button to both save any changes and restart the panel. ***Remember that you will need to navigate to the System Settings page and configure the connection to a target Master.***
14. After the panel restarts, return to the Wireless Settings page to verify the Link Quality and Signal Strength:
    - The descriptions are: **None**, **Poor**, **Fair**, **Good**, **Very Good**, and **Excellent**.

NOTE

The signal strength field provides some descriptive text regarding the strength of the connection to a Wireless Access Point. If there is no signal or no IP Address displayed; configuration of your network could be required.

Refer to the NXA-WAP200G Instruction Manual for more detailed setup and configuration procedures.

Configuring Multiple Wireless Moderos To Communicate To a Target WAP200G

1. For each communicating touch panel, complete all of the steps outlined within the previous *Configuring the Modero's wireless card for secured access to a WAP200G* section on page 48.
2. Navigate back to the Wireless Settings page on each panel.
3. Verify that all communicating Modero panels are using the same **SSID**, **encryption level**, **Default Key #**, and an identical **Current Key value**.
   - As an example, all panels should be set to Default Key **#1** and be using **aa:bb:cc**..as the Current Key string value. This same Key value and Current Key string should be used on the target WAP.
4. Repeat steps 1 - 3 on each panel. **Using the same passphrase, generates the same key for all communicating Modero panels.**

Step 3: Choose a Master Connection Mode

The panel requires you establish the type of connection you want made between it and your master.

In the *Protected Setup* page:

1. Select *System Settings.*
2. Select *Type* to toggle between the Master Connection Types *USB* and *Ethernet*.
   - A USB connection is a direct connection from the panel's mini-USB port to a corresponding USB port on the PC (acting as a Virtual Master).
   - A Wireless Ethernet connection involves indirect communication from the panel to a Master via a wireless connection to the network.

WARNING

It is recommended that firmware KIT files only be transferred over a direct connection and only when the panel is connected to a power supply. If battery power or wireless connection fails during a firmware upgrade, the panel flash file system may become corrupted.

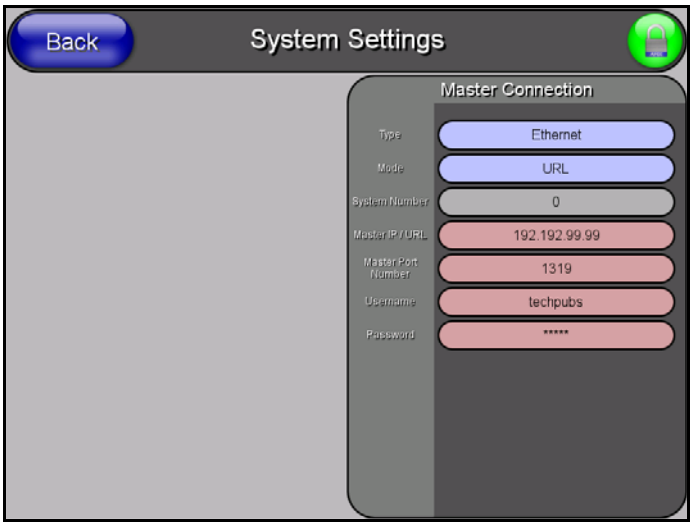


FIG. 36 System Settings page

USB

NetLinx Studio can be setup to run a Virtual Master where the PC acts as the Master by supplying its own IP Address for communication to the panel. For a PC to establish a USB connection with a Modero panel, it must have the AMX USBLAN driver installed.

NOTE

The AMX USBLAN driver is included with both NetLinx Studio2 and TPDesign4, and can also be downloaded as a stand-alone application from www.amx.com.

Prepare your PC for USB communication with the panel

If you haven't already done so, download and install the latest versions of NetLinx Studio2 and TPDesign4 (from www.amx.com), and restart your PC.

Configure the panel for USB communication

The first time the panel is connected to the PC it is detected as a new USB hardware device, and the correct (panel-specific) USBLAN driver must be associated to it manually. Each time thereafter, the panel is recognized as a unique USBLAN device, and the association to the driver is handled automatically.

1. Connect the PS4.4 power connector to the panel (or docking station if the panel is already installed) to supply power.
2. Press and hold the two lower external pushbuttons on either side of the panel simultaneously for 3 seconds to access the Setup page.
3. In the Protected Settings page, select **System Settings** to open the System Settings page (FIG. 37).
4. Toggle the blue *Type* field (***from the Master Connection section***) until the choice cycles to **USB**.

   Refer to the *System Settings Page* section on page 86 for information about the fields on this page.

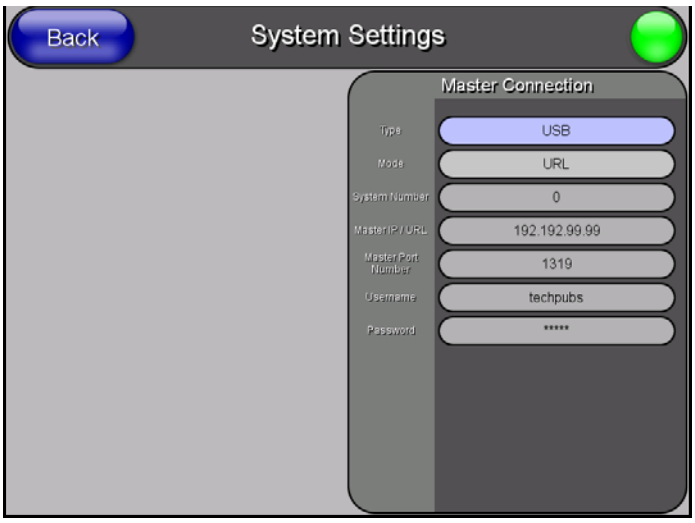


FIG. 37 System Settings page - USB Connection

5. Press the **Back** button to return to the Protected Setup page.
6. Press **Reboot** to save changes and restart the panel.
7. When the panel powers up and displays the first panel page, insert the mini-USB connector into the Program Port on the panel.

   It may take a minute for the panel to detect the new connection and send a signal to the PC (*indicated by a green System Connection icon*).
   The first time the panel is recognized by the PC as a new USB device, a USB driver installation popup window (FIG. 38) is displayed. This window notifies you that the panel has been detected as a USB device, and the appropriate USB driver is being installed to establish communication with the panel. It also indicates that the AMX USBLAN driver does not contain a Microsoft® digital signature.

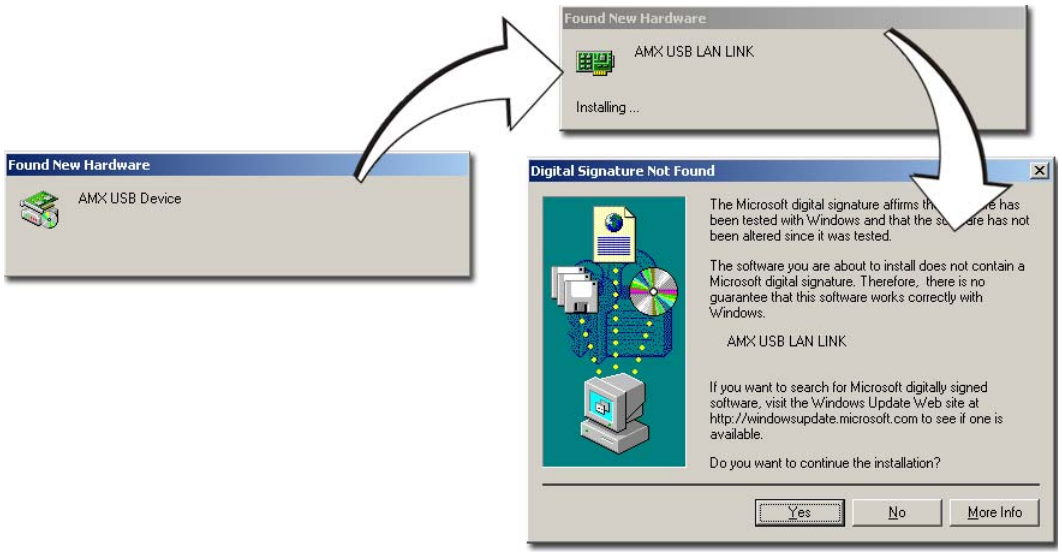


FIG. 38 USB driver installation popup window

8. Click **Yes** to proceed with the driver installation.

   Once the installation is complete, the panel and PC are ready to communicate via USB.

9. Navigate back to the *System Settings* page.

Configure a Virtual NetLinx Master using NetLinx Studio

A Virtual NetLinx Master (VNM) is used when the target panel is not connected to a physical NetLinx Master. In this situation, the PC takes on the functions of a Master via a Virtual NetLinx Master. This connection is made by either using the PC's Ethernet Address (via TCP/IP using a known PC's IP Address as the Master) or using a direct mini-USB connection to communicate directly to the panel.

Before beginning:

1. Verify the panel has been configured to communicate via USB within the System Settings page and that the USB driver has been properly configured. Refer to the previous section for more information.
2. In NetLinx Studio, select **Settings > Master Communication Settings**, from the Main menu to open the Master Communication Settings dialog (FIG. 39).

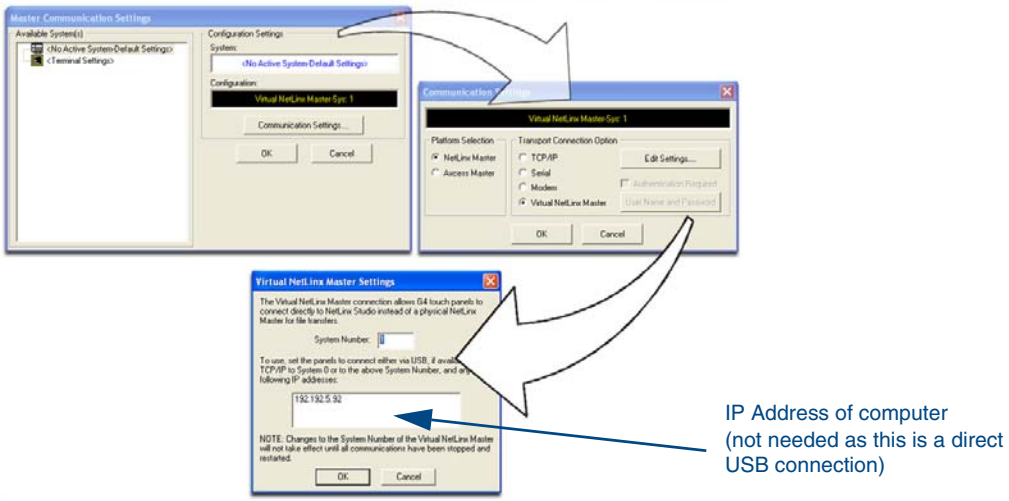


FIG. 39 Assigning Communication Settings for a Virtual Master

3. Click the **Communications Settings** button to open the *Communications Settings* dialog.
4. Click the **NetLinx Master** radio button (*from the Platform Selection section*).
5. Click the **Virtual Master** radio button (*from the Transport Connection Option section*).
6. Click the **Edit Settings** button to open the *Virtual NetLinx Master Settings* dialog (FIG. 39).
7. Enter the System number (default is **1**).
8. Click **OK** to close all open dialogs and save your settings.
9. Click the **OnLine Tree** tab in the Workspace window to view the devices on the Virtual System.
10. Right-click on *Empty Device Tree/System* and select **Refresh System** to re-populate the list.
    The panel will not appear as a device below the virtual system number (in the Online Tree tab) until both the system number (default = 1) is entered into the Master Connection section of the System Settings page and the panel is restarted.
    - The Connection status turns green after a few seconds to indicate an active USB connection to the PC (Virtual Master).
    - If the System Connection icon does not turn green, check the USP connection and communication settings and refresh the system.

Ethernet

1. When using *Ethernet*, press the listed *Mode* to toggle through the available connection modes:

Connection Modes

Mode	Description	Procedures
Auto	The device connects to the first master that responds. This setting requires you set the System Number.	Setting the System Number: 1. Select the *System Number* to open the keypad. 2. Set your System Number select **Done**.
URL	The device connects to the specific IP of a master via a TCP connection. This setting requires you set the Master's IP.	Setting the Master IP: 1. Select the *Master IP* number to the keyboard. 2. Set your Master IP and select **Done**.
Listen	The device "listens" for the master to initiate contact. This setting requires you provide the master with the device's IP.	Confirm device IP is on the Master URL list. You can set the Host Name on the device and use it to locate the device on the master. Host Name is particularly useful in the DHCP scenario where the IP address can change.

2. Select the *Master Port Number* to open the keypad and change this value. The default setting for the port is *1319*.
3. Set your Master Port and select **Done**.

If you have enabled password security on your master you need to set the username and password within the device.

4. Select the blank field *Username* to open the keyboard.
5. Set your Username and select **Done**.
6. Select the blank field *Password* to open the keyboard.
7. Set your Password and select **Done**.
8. Press the **Back** button to return to the *Protected Setup* page.
9. Press the **Reboot** button to reboot device and confirm changes.

Master Connection to a Virtual Master via Ethernet

NOTE

When configuring your panel to communicate with a Virtual Master (on your PC) via wireless Ethernet, the Master IP/URL field must be configured to match the IP Address of the PC and make sure to use the Virtual System value assigned to the Virtual Master within NetLinx Studio.

Before beginning:

1. Verify the panel has been configured to communicate with the Wireless Access Point and verify the signal strength quality bargraph is On.
2. Launch NetLinx Studio 2.x (default location is **Start > Programs > AMX Control Disc > NetLinx Studio 2 > NetLinx Studio 2**).
3. Select **Settings > Master Communication Settings**, from the Main menu to open the Master Communication Settings dialog (FIG. 40).

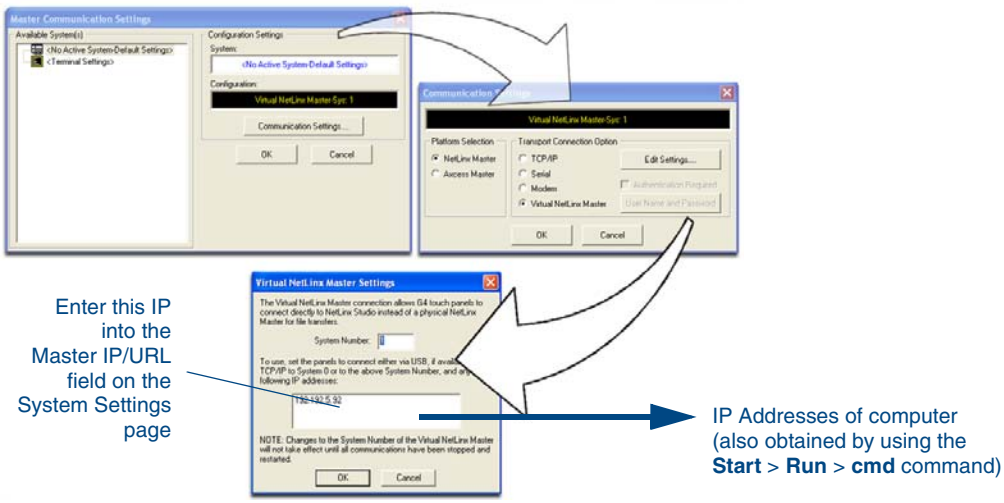


FIG. 40 Assigning Communication Settings and TCP/IP Settings for a Virtual Master

4. Click the **Communications Settings** button to open the Communications Settings dialog.
5. Click on the **NetLinx Master** radio button (*from the Platform Selection section*) to indicate that you are working as a NetLinx Master.
6. Click on the **Virtual Master** radio box (*from the Transport Connection Option section*) to indicate you are wanting to configure the PC to communicate with a panel. Everything else such as the Authentication is greyed-out because you are not going through the Master's UI.
7. Click the **Edit Settings** button (*on the Communications Settings dialog*) to open the Virtual NetLinx Master Settings dialog (FIG. 40).
8. From within this dialog enter the System number (**default is 1**) and note the IP Address of the target PC being used as the Virtual Master. This IP Address can also be obtained by following these procedures:
   - On your PC, click **Start > Run** to open the Run dialog.
   - Enter **cmd** into the Open field and click **OK** to open the command DOS prompt.
   - From the **C:\>** command line, enter **ipconfig** to display the IP Address of the PC. This information is entered into the *Master IP/URL* field on the panel.
9. Click **OK** three times to close the open dialogs, save your settings, and return to the main NetLinx Studio application.
10. Click the **OnLine Tree** tab in the Workspace window to view the devices on the Virtual System. *The default System value is **one***.
11. Right-click on the *Empty Device Tree/System* entry and select **Refresh System** to re-populate the list.
12. Connect the terminal end of the PS4.4 power cable to the 12 VDC power connector on the side of the stand-alone touch panel.

13. After the panel powers-up, press and hold the two lower buttons on both sides of the display (**for 3 seconds**) to continue with the setup process and proceed to the Setup page.
14. Select **Protected Setup > System Settings** (located on the lower-left) to open the System Settings page (FIG. 41).

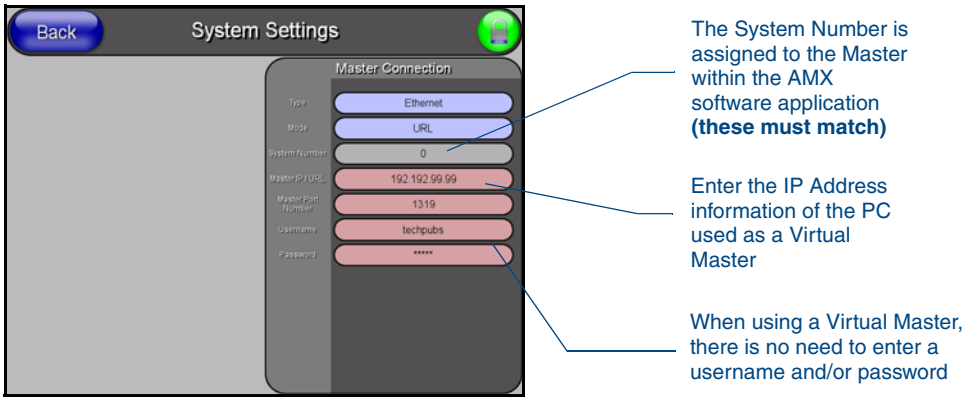


FIG. 41 Sample System Settings page (for Virtual Master communication)

15. Press the blue *Type* field (***from the Master Connection section***) until the choice cycles to the word **Ethernet.**
16. Press the *Mode* field until the choice cycles to the word **URL**.
    - By selecting **URL**, the System Number field becomes read-only (grey) because the panel pulls this value directly from the communicating target Master (virtual or not). A Virtual Master system value can be set within the active AMX software applications such as: NetLinx Studio, TPD4, or IREdit.
17. Press the *Master IP/URL* field to open a Keyboard and enter the IP Address of the PC used as the Virtual Master.
18. Click **Done** to accept the new value and return to the System Settings page.
19. Do not alter the Master Port Number value (*this is the default value used by NetLinx*).
20. Press the **Back** button to open the Protected Setup page.
21. Press the on-screen **Reboot** button to both save any changes and restart the panel.

Using G4 Web Control to Interact with a G4 Panel

The G4 Web Control feature allows you to use a PC to interact with a G4 enabled panel via the web. This feature works in tandem with the new browser-capable NetLinx Security firmware update (***build 300 or higher***). G4 Web Control is only available with the latest Modero panel firmware.

Refer to the *G4 Web Control Page* section on page 108 for more detailed field information.

NOTE

*Verify your NetLinx Master (ME260/64 or NI-Series) has been installed with the latest firmware KIT file from **www.amx.com**. Refer to your NetLinx Master instruction manual for more detailed information on the use of the new web-based NetLinx Security.*

1. Press and hold the two lower buttons on both sides of the display for **3 seconds** to open the Setup page.
2. Press the **Protected Setup** button (located on the lower-left of the panel page) to open the Protected Setup page and display an on-screen keypad.
3. Enter ***1988*** into the Keypad's password field (***1988*** *is the default password*).

NOTE

Clearing Password #5, from the initial Password Setup page, removes the need for you to enter the default password before accessing the Protected Setup page.

4. Press **Done** when finished.
5. Press the **G4 WebControl** button to open the G4 Web Control page (FIG. 42).

FIG. 42 G4 Web Control page

6. Press the **Enable/Enabled** button until it toggles to **Enabled** (*light blue color*).
7. The *Network Interface Select* field is read-only and displays the method of communication to the web.
   - **Wireless** is used when a wireless card is detected within the internal card slot. This method provides an indirect communication to the web via a pre-configured Wireless Access Point.

NOTE

*The Network Interface Select field is read-only and defaulted to **Wireless (since there is no Ethernet cable connection)**.*

8. Press the *Web Control Name* field to open the Web Name keyboard.
9. From the Web Name keyboard, enter a unique alpha-numeric string to identify this panel. This information is used by the NetLinx Security Web Server to display on-screen links to the panel. *The on-screen links use the IP Address of the panel and not the name for communication* (FIG. 43).
10. Press **Done** after you are finished assigning the alpha-numeric string for the Web Control name.
11. Press the *Web Control Password* field to open the Web Password keyboard.

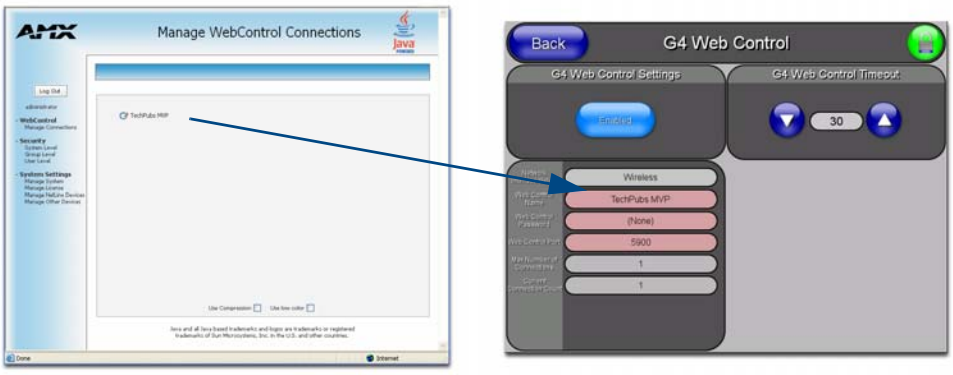


FIG. 43 Sample relationship between G4 Web Control and Mange WebControl Connections window

12. From the Web Password keyboard, enter a unique alpha-numeric string to be assigned as the G4 Authentication session password associated with VNC web access of this panel.
13. Press **Done** after you are finished assigning the alpha-numeric string for the Web Control password.
14. Press the *Web Control Port* field to open the Web Port Number keypad.
15. Within the keypad, enter a unique numeric value to be assigned to the port the VNC Web Server is running on. The default value is ***5900***.
16. Press **Done** when you are finished entering the value. *The remaining fields within the G4 Web Control Settings section of this page are read-only and cannot be altered.*
17. Press the **Up/Down** arrows on either sides of the G4 Web Control *Timeout* field to increase or decrease the amount of time the panel can remain idle (***no cursor movements***) before the session is closed and the user is disconnected.
18. Press the **Back** button to open the Protected Setup page.
19. Press the on-screen **Reboot** button to save any changes and restart the panel.

NOTE

Verify your NetLinx Master's IP Address and System Number have been properly entered into the Master Connection section of the System Settings page.

Using your NetLinx Master to control the G4 panel

Refer to your particular NetLinx Master's instruction manual for detailed information on how to download the latest firmware from **www.amx.com**. This firmware build enables SSL certificate identification and encryption, HTTPS communication, ICSP data encryption, and disables the ability to alter the Master security properties via a TELNET session.

NOTE

In order to fully utilize the SSL encryption, your web browser should incorporate the an encryption feature. This encryption level is displayed as a Cipher strength.

Once the Master's IP Address has been set through NetLinx Studio version 2.x or higher:

1. Launch your web browser.
2. Enter the IP Address of the target Master (***ex: http://198.198.99.99***) into the web browser's *Address* field.
3. Press the **Enter** key on your keyboard to begin the communication process between the target Master and your computer.
   - Initially, the Master Security option is disabled (from within the **System Security** page) and no username and password is required for access or configuration.
   - Both HTTP and HTTPS Ports are enabled by default (via the **Manage System > Server** page).

- If the Master has been previously configured for secured communication, click **OK** to accept the AMX SSL certificate (*if SSL is enabled*) and then enter a valid username and password into the fields within the *Login* dialog.

4. Click **OK** to enter the information and proceed to the Master's Manage WebControl Connections window.
5. This Manage WebControl Connections page (FIG. 44) is accessed by clicking on the **Manage connections** link (*within the Web Control section within the Navigation frame*). Once activated, this page displays links to G4 panels running the latest G4 Web Control feature (*previously setup and activated on the panel*).

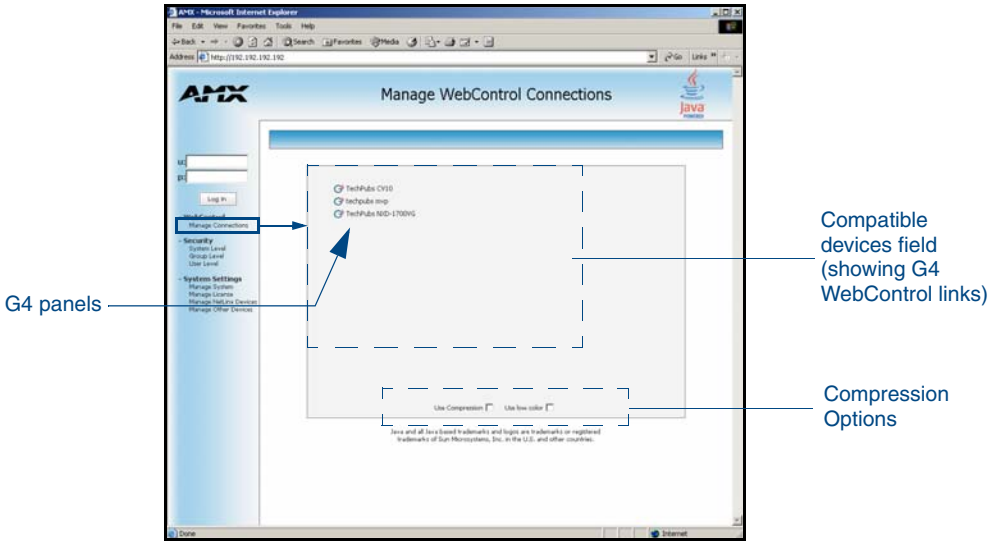


FIG. 44 Manage WebControl Connections page (populated with compatible panels)

6. Click on the G4 panel name link associated with the target panel. A secondary web browser window appears on the screen (FIG. 45).

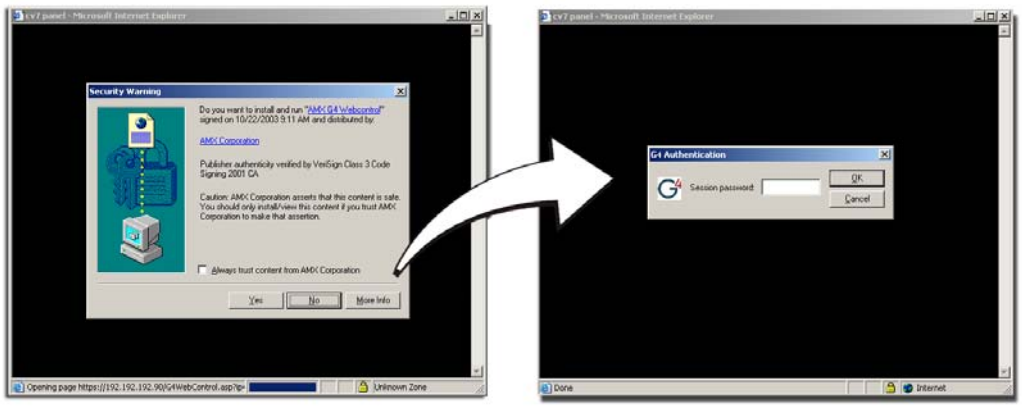


FIG. 45 Web Control VNC installation and Password entry screens

7. Click **Yes** from the Security Alert popup window to agree to the installation of the G4 WebControl application on your computer. This application contains the necessary Active X and VNC client applications necessary to properly view and control the panel pages from your computer.

NOTE

The G4 Web Control application is sent by the panel to the computer that is used for communication. Once the application is installed, this popup will no longer appear. This popup will only appear if you are connecting to the target panel using a different computer.

8. In some cases, you might get a *Connection Details* dialog (FIG. 46) requesting a VNC Server IP Address. This is the IP Address not the IP of the Master but of the target touch panel. Depending on which method of communication you are using, it can be found in either the:
   - **Wired Ethernet** - System Settings > IP Settings section within the *IP Address* field.
   - **Wireless** - Wireless Settings > IP Settings section within the *IP Address* field.
   - If you do not get this field continue to step 9.

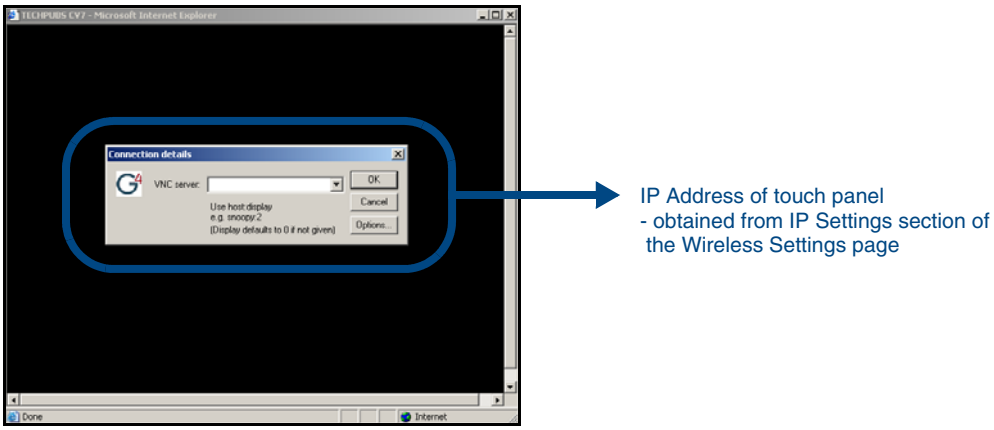


FIG. 46 Connection Details dialog

9. If a WebControl password was setup on the G4 WebControl page, a G4 Authentication Session password dialog box appears on the screen within the secondary browser window.
10. Enter the Web Control session password into the *Session Password* field (FIG. 46). *This password was previously entered into the Web Control Password field within the G4 Web Control page on the panel.*
11. Click **OK** to send the password to the panel and begin the session. A confirmation message appears stating *"Please wait, Initial screen loading..".*

The secondary window then becomes populated with the same G4 page being displayed on the target G4 panel. A small circle appears within the on-screen G4 panel page and corresponds to the location of the mouse cursor. A left-mouse click on the computer-displayed panel page equates to an actual touch on the target G4 panel page.

Upgrading Modero Firmware

Overview

Before beginning the Upgrade process:

- Setup and configure your NetLinx Master. Refer to the your particular NetLinx Master Instruction Manual for detailed setup procedures.
- Calibrate and prepare the communication pages on the Modero panel for use. Refer to the *Panel Calibration* section on page 39.

NOTE

The latest NXD-700Vi firmware kit file is now panel-specific.
Only NXD-700Vi firmware should be loaded onto this specific panel type.
This new firmware also provides both backwards compatibility with the previous 802.11b cards and new security protocols for the new 802.11g wireless CF card.

- Refer to the NetLinx Studio version 2.x Help file for more information on uploading files via Ethernet.
- Configure your panel for either direct connect or wireless communication. Refer to the *Configuring Communication* section on page 41 for more information.

WARNING

It is recommended that firmware Kit files only be transferred over a direct Ethernet connection and only when the panel is connected to a power supply.
If battery power or wireless connection fails during a firmware upgrade, the panel flash file system may become corrupted.

The process of updating firmware involves the use of a communicating NetLinx Master. The required steps for updating firmware to a Modero panel are virtually identical to those necessary for updating Kit files to a NetLinx Master (*except the target device is a panel instead of a Master*). Refer to either your Master's literature or Studio 2.x Help file for those procedures.

WARNING

A touch panel which is not using a valid username and password will not be able to communicate with a secured Master. If you are updating the firmware on or through a panel which is not using a username or password field, you must first remove the Master Security feature to establish an unsecured connection.

Upgrading the Modero Firmware via the USB port

Before beginning with this section, verify your panel is both powered and the Type-A USB connector is securely inserted into the PC's USB port. **The panel must be powered-on before connecting the mini-USB connector to the panel.**

WARNING

Establishing a USB connection between the PC and the panel, prior to installing the USB Driver will cause a failure in the USB driver installation.

Step 1: Configure the panel for a USB Connection Type

1. After the installation of the USB driver has been completed; confirm the proper installation of the large Type-A USB connector to the PC's USB port, and restart your machine.
2. After the panel powers-up, press and hold the grey Front Setup Access button (**for 3 seconds**) to continue with the setup process and proceed to the Setup page.
3. Select **Protected Setup > System Settings** (located on the lower-left) to open the System Settings page.
4. Toggle the blue *Type* field (***from the Master Connection section***) until the choice cycles to **USB**.

NOTE

ALL fields are then greyed-out and read-only, but still display any previous network information.

5. Press the **Back** button on the touch panel to return to the Protected Setup page.
6. Press the on-screen **Reboot** button to both save any changes and **restart the panel.** *Remember that the panel's connection type must be set to **USB** prior to rebooting the panel and prior to inserting the USB connector.*
7. **ONLY AFTER** the unit displays the first panel page, **THEN** insert the mini-USB connector into the Program Port on the panel. It may take a minute for the panel to detect the new connection and send a signal to the PC (*indicated by a green System Connection icon*).
   - If a few minutes have gone by and the System Connection icon still does not turn green, complete the procedures in the following section to setup the Virtual Master and refresh the System from the Online Tree. This action sends out a request to the panel to respond and completes the communication (turning the System Connection icon green).
8. Navigate back to the System Settings page.

Step 2: Prepare NetLinx Studio for communication via the USB port

1. Launch NetLinx Studio 2.x (default location is **Start > Programs > AMX Control Disc > NetLinx Studio 2 > NetLinx Studio 2**).
2. Select **Settings > Master Communication Settings**, from the Main menu to open the Master Communication Settings dialog (FIG. 47).

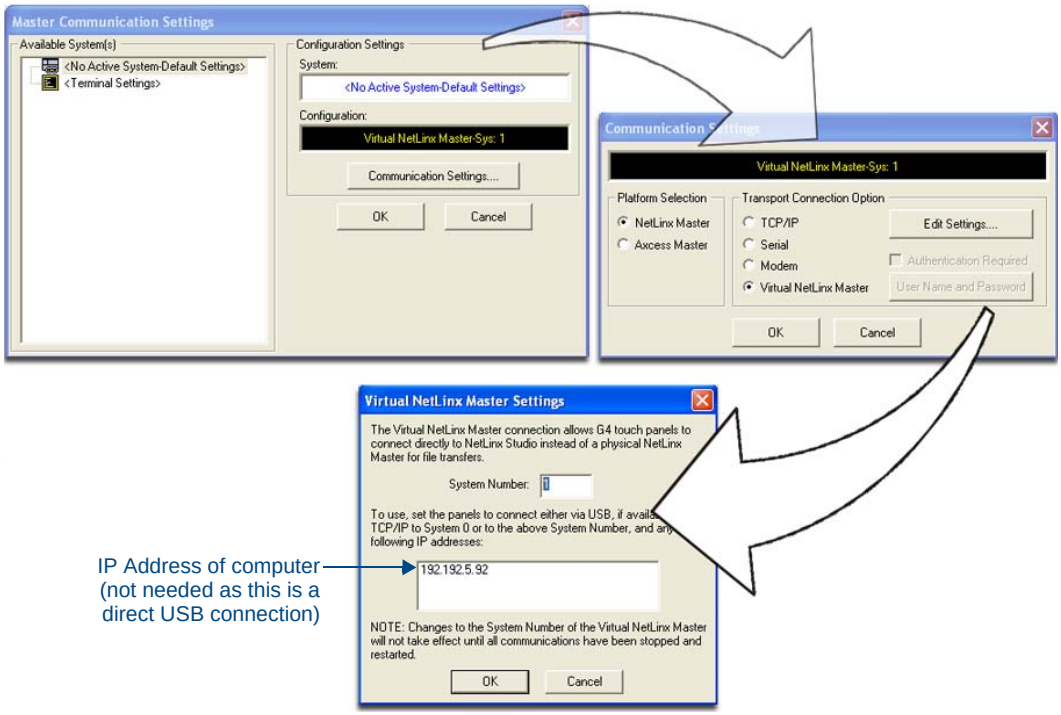


FIG. 47 Assigning Communication Settings for a Virtual Master

3. Click the **Communications Settings** button to open the *Communications Settings* dialog.
4. Click on the **NetLinx Master** radio button (*from the Platform Selection section*) to indicate that you are working as a NetLinx Master.
5. Click on the **Virtual Master** radio box (*from the Transport Connection Option section*) to indicate you are wanting to configure the PC to communicate directly with a panel. Everything else such as the Authentication is greyed-out because you are not going through the Master's UI.

6. Click the **Edit Settings** button (*on the Communications Settings dialog*) to open the *Virtual NetLinx Master Settings* dialog (FIG. 47).
7. From within this dialog enter the System number (default is **1**).
8. Click **OK** three times to close the open dialogs, save your settings, and return to the main NetLinx Studio application.
9. Click the **OnLine Tree** tab in the Workspace window to view the devices on the Virtual System. *The default System value is one*.
10. Right-click on the *Empty Device Tree/System* entry and select **Refresh System** to re-populate the list. ***The panel will not appear as a device below the virtual system number (in the Online Tree tab) until both the system number used in step 7 for the Virtual NetLinx Master (VNM) is entered into the Master Connection section of the System Settings page and the panel is restarted.***

NOTE

If the G4 panel does not appear, refer to the Appendix C: Troubleshooting section on page 207 *for more information.*

Step 3: Confirm and Upgrade the firmware via the USB port

Use the CC-USB Type-A to Mini-B 5-wire programming cable (**FG10-5965**) to provide communication between the mini-USB Program port on the touch panel and the PC. This method of communication is used to transfer firmware Kit files and TPD4 touch panel files.

NOTE

A mini-USB connection is only detected after it is installed onto an active panel. Connection to a previously powered panel which then reboots, allows the PC to detect the panel and assign an appropriate USB driver.

1. Verify this direct USB connection (Type-A on the panel to mini-USB on the panel) is configured properly using the steps outlined in the previous two sections.
2. With the panel already configured for USB communication and the Virtual Master setup within NetLinx Studio, its now time to verify the panel is ready to receive files.
3. After the Communication Verification dialog window verifies active communication between the Virtual Master and the panel, click the **OnLine Tree** tab in the Workspace window (FIG. 48) to view the devices on the Virtual System. *The default System value is one*.
4. Right-click on the System entry (FIG. 48) and select **Refresh System** to re-populate the list. Verify the panel appears in the **OnLine Tree** tab of the Workspace window. *The default Modero panel value is 10001*.

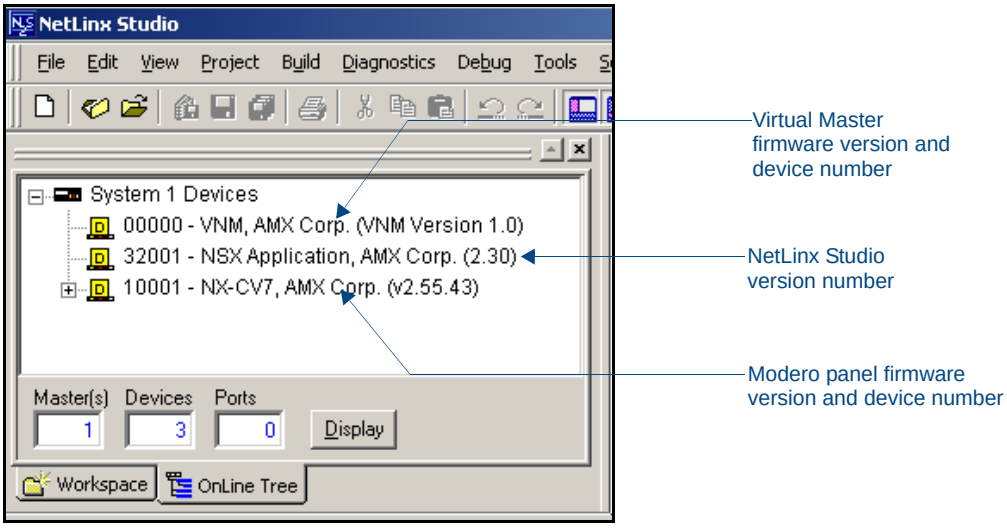


FIG. 48 NetLinx Workspace window (showing the panel connection via a Virtual NetLinx Master)

NOTE

The latest NXD-700Vi firmware kit file is now panel-specific.
Only NXD-700Vi firmware should be loaded onto this specific panel type.
This new firmware also provides both backwards compatibility with the previous 802.11b cards and new security protocols for the new 802.11g wireless CF card.

5. If the panel firmware being used is not current, download the latest Kit file by first logging in to **www.amx.com** and then navigate to **Tech Center > Firmware Files** and from within the **Modero** section of the web page locate your Modero panel.
6. Click on the desired Kit file link and after you've accepted the Licensing Agreement, verify you have downloaded the Modero Kit file to a known location.
7. From within Studio, select **Tools > Firmware Transfers > Send to NetLinx Device** from the Main menu to open the Send to NetLinx Device dialog (**B** in FIG. 49). Verify the panel's System and Device number values match those values listed within the System folder in the **OnLine Tree** tab of the Workspace window (**A** in FIG. 49).

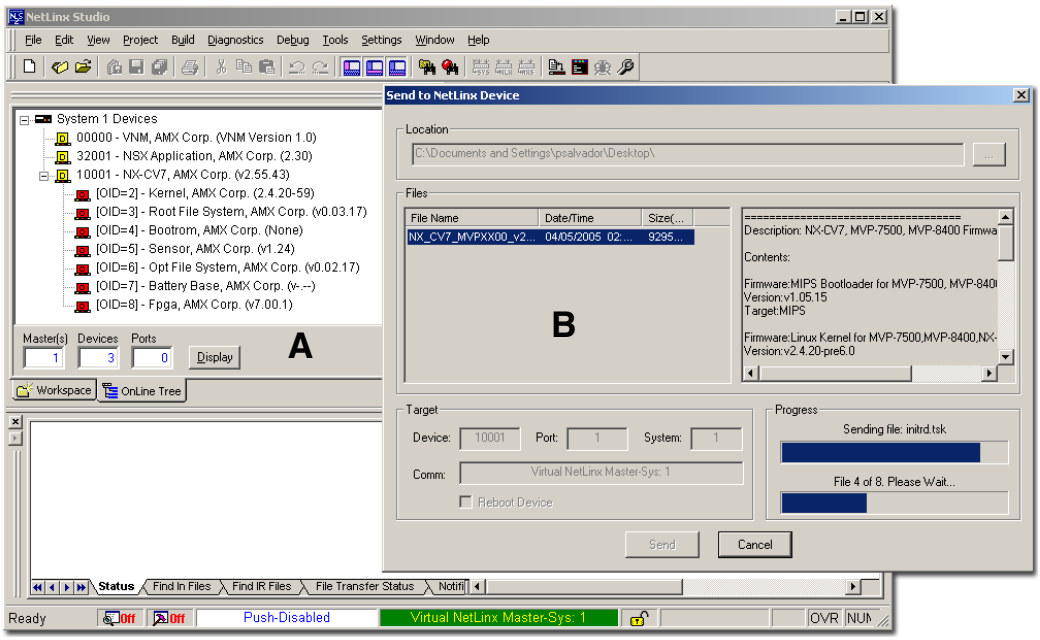


FIG. 49 Using USB for a Virtual Master transfer

8. Select the panel's Kit file from the **Files** section.
9. Enter the **Device** value associated with the panel and the **System** number associated with the Master (*listed in the OnLine Tree tab of the Workspace window*). *The Port field is greyed-out.*
10. Click the **Reboot Device** checkbox. This causes the touch panel to reboot after the firmware update process is complete. *The reboot of the panel can take up 30 seconds after the firmware process has finished.*
11. Click **Send** to begin the transfer. The file transfer progress is indicated on the bottom-right of the dialog (**B** in FIG. 49).
12. As the panel is rebooting, temporarily unplug the USB connector on the panel until the panel has completely restarted.
13. Once the first panel page has been displayed, reconnect the USB connector to the panel.
14. Right-click the associated System number and select **Refresh System**. This causes a refresh of all project systems, establishes a new connection to the Master, and populates the System list with devices on your particular system.
15. Confirm the panel has been properly updated to the correct firmware version.

Upgrading the Modero Firmware via Ethernet (IP Address)

Before beginning with this section, verify that your panel is powered and connected to the NetLinx Master through an Ethernet connection (direct or wireless).

Step 1: Prepare the Master for communication via an IP

1. Obtain the IP Address of the NetLinx Master from your System Administrator. If you do not have an IP Address for the Master, refer to your particular Master's instruction manual for more information on obtaining this IP Address using NetLinx Studio 2.x.
   - From the **Online Tree** tab of the Workspace window, select the NetLinx Master.
   - Follow steps outlined in either the *Obtaining or Assigning the Master's IP Address* sections from your particular NetLinx Master instruction manual to use an address.
   - Note the IP Address and Gateway information.
2. Launch NetLinx Studio 2.x (default location is **Start > Programs > AMX Control Disc > NetLinx Studio 2 > NetLinx Studio 2**).
3. Select **Settings > Master Communication Settings** from the Main menu to open the Master Communication Settings dialog (FIG. 50).

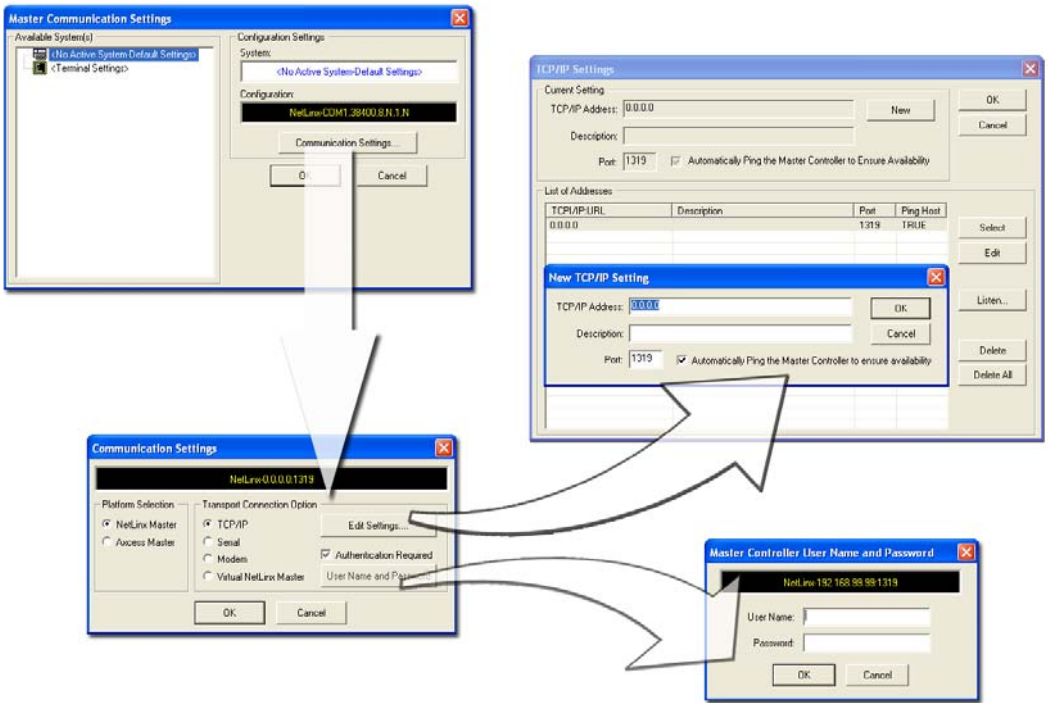


FIG. 50 Assigning Master Communication Settings and TCP/IP Settings

4. Click the **Communications Settings** button to open the Communications Settings dialog.
5. Click on the **NetLinx Master** radio button (*from the Platform Selection section*) to indicate you are working with a NetLinx Master (such as the NXC-ME260/64 or NI-Series of Integrated Controllers).
6. Click on the **TCP/IP** radio button (*from the Transport Connection Option section*) to indicate you are connecting to the Master through an IP Address.
7. Click the **Edit Settings** button (*on the Communications Settings dialog*) to open the TCP/IP Settings dialog (FIG. 50). This dialog contains a series of previously entered IP Address/URLs and their associated names, all of which are stored within Studio and are user-editable.
8. Click the **New** button to open the New TCP/IP Settings dialog where you can enter both a previously obtained DHCP or Static IP Address and an associated description for the connection into their respective fields.

9. Place a checkmark within the *Automatically Ping the Master Controller to ensure availability* radio box to make sure the Master is initially responding online before establishing full communication.
10. Click **OK** to close the current New TCP/IP Settings dialog and return to the previous TCP/IP Settings dialog where you must locate your new entry within the List of Addresses section.
11. Click the **Select** button to make that the currently used IP Address communication parameter.
12. Click **OK** to return to the Communications Settings dialog and place a checkmark within the *Authentication Required* radio box if your Master has been previously secured with a username/password.
13. Click on the **Authentication Required** radio box (if the Master is secured) and then press the **User Name and Password** button to open the Master Controller User Name and Password dialog.
14. Within this dialog, you must enter a previously configured username and password (with sufficient rights) before being able to successfully connect to the Master.
15. Click **OK** to save your newly entered information and return to the previous Communication Settings dialog where you must click **OK** again to begin the communication process to your Master.

If you are currently connected to the assigned Master, a popup asks whether you would want to temporarily stop communication to the Master and apply the new settings.

16. Click **Yes** to interrupt the current communication from the Master and apply the new settings.
17. Click **Reboot** (*from the Tools > Reboot the Master Controller dialog*) and wait for the System Master to reboot. *The STATUS and OUTPUT LEDs should begin to alternately blink during the incorporation. Wait until the STATUS LED is the only LED to blink.*
18. Press **Done** once until the *Master Reboot Status* field reads **Reboot of System Complete**.
19. Click the **OnLine Tree** tab in the Workspace window to view the devices on the System. *The default System value is one (1).*
20. Right-click the associated System number and select **Refresh System**. This establishes a new connection to the specified System and populates the list with devices on that system. *The communication method is then highlighted in green on the bottom of the NetLinx Studio window.*

Step 2: Prepare the Panel For Communication Via an IP

1. Press the blue *Type* field (*from the Master Connection section*) until the choice cycles to the word **Ethernet**.
2. Press the blue *Mode* field until the choice cycles to the word **URL**.
   - By selecting **URL**, the System Number field becomes read-only (grey) because the panel pulls this value directly from the communicating target Master (virtual or not). A Virtual Master system value can be set within the active AMX software applications such as: NetLinx Studio, TPD4, or IREdit.
3. Press the red *Master IP/URL* field to open a Keyboard and enter the NetLinx Master's IP Address **(obtained from the Diagnostics - Networking Address dialog of the NetLinx Studio application)**.
4. Click **Done** to accept the new value and return to the System Configuration page.
5. Do not alter the Master Port Number value (*this is the default value used by NetLinx*).
6. Press the **Back** button to return to the Protected Setup page and press the on-screen **Reboot** button to restart the panel and save any changes.

Step 3: Verify and Upgrade the Panel Firmware Via an IP

1. Click the **OnLine Tree** tab in the Workspace window to view the devices on the System. *The default System value is one.*
2. Right-click the associated System number (from the Workspace window) and select **Refresh System** to detect of all devices on the current system, establish a new connection to the Master, and refresh the System list with devices on that system.
3. After the Communication Verification dialog window verifies active communication between the PC and the Master, verify the panel appears in the **OnLine Tree** tab of the Workspace window (see FIG. 48 on page 65). *The default Modero panel value is 10001.*

4. If the panel firmware being used is not current, download the latest Kit file by first logging in to **www.amx.com** and then navigate to **Tech Center > Firmware Files** and from within the **Modero** section of the web page locate your Modero panel.

NOTE

The latest NXD-700Vi firmware kit file is now panel-specific.
Only NXD-700Vi firmware should be loaded onto this specific panel type.
This new firmware also provides both backwards compatibility with the previous 802.11b cards and new security protocols for the new 802.11g wireless CF card.

5. Click on the desired Kit file link and after you've accepted the Licensing Agreement, verify you have downloaded the Modero Kit file to a known location.
6. From within Studio, select **Tools > Firmware Transfers > Send to NetLinx Device** from the Main menu to open the Send to NetLinx Device dialog (FIG. 51). Verify the panel's System and Device number values match those values listed within the System folder in the **OnLine Tree** tab of the Workspace window.

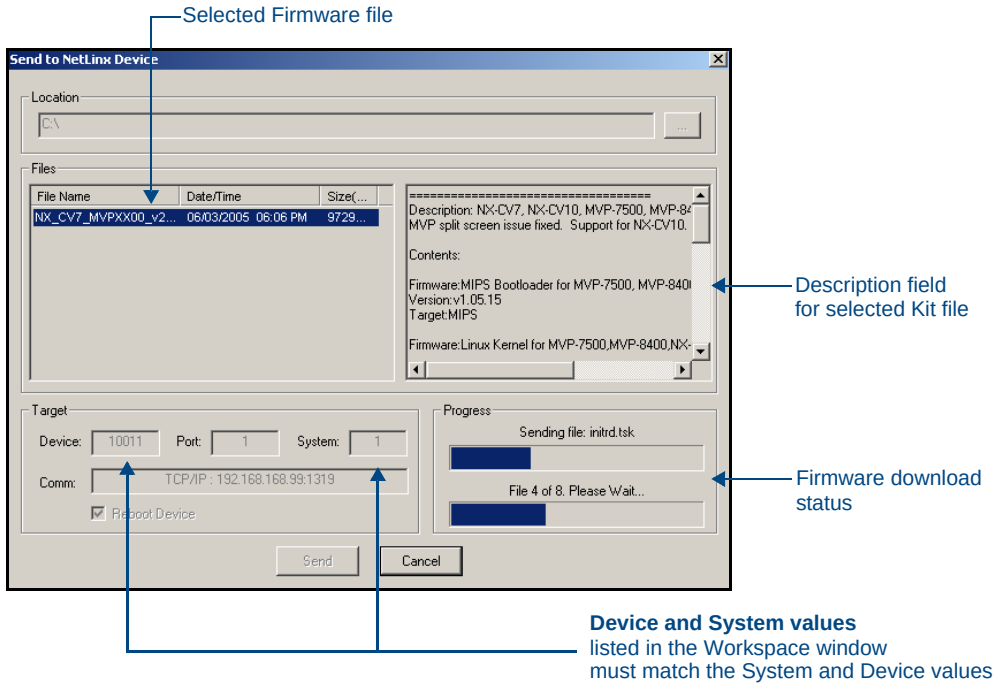


FIG. 51 Send to NetLinx Device dialog (showing Modero firmware update via IP)

Select the panel's Kit file from the **Files** section (FIG. 51).

7. Enter the **Device** value associated with the panel and the **System** number associated with the Master (*listed in the OnLine Tree tab of the Workspace window*). *The Port field is greyed-out.*
8. Click the **Reboot Device** checkbox. This causes the touch panel to reboot after the firmware update process is complete. *The reboot of the panel can take up 30 seconds after the firmware process has finished.*
9. Click **Send** to begin the transfer. The file transfer progress is indicated on the bottom-right of the dialog (FIG. 51).
10. Click **Close** (*after the panel reboots*) to return to the main program.
11. Right-click the associated System number and select **Refresh System**. This causes a refresh of all project systems, establishes a new connection to the Master, and populates the System list with devices on your particular system.
12. Confirm the panel has been properly updated to the correct firmware version.

Firmware Pages and Descriptions

This section describes each firmware page and their specific functional elements.

Setup Navigation Buttons

These Setup Navigation Buttons (FIG. 52) appear on the left of the panel screen when the Setup page is currently active.

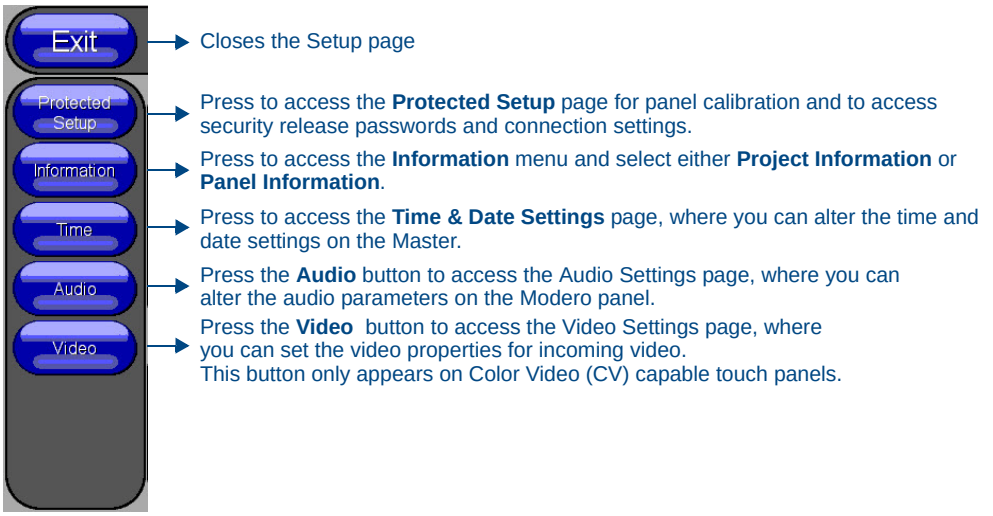


FIG. 52 Setup Navigation Buttons

Protected Setup Page

This button opens the Protected Setup page which centers around the properties used by the panel to properly communicate with the NetLinx Master. Refer to both the *Protected Setup Navigation Buttons* section on page 83 and the *Protected Setup Page* section on page 71 for more detailed information.

Setup Page

This page (FIG. 53) centers around basic Modero panel properties such as: Connection Status of the panel, Display Timeout, Inactivity Page Flip Time, Inactivity page file, and the Panel Brightness.

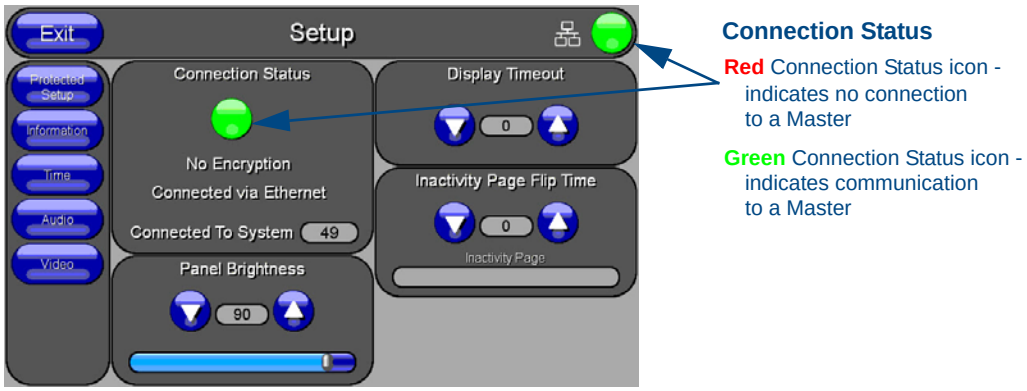


FIG. 53 Setup page

The elements of the Setup page are described in the table below:

Setup Page Elements	
Exit:	Returns you to the Main touch panel page. In this case, the previous page is the default Main page.
Connection Status icon:	This visual display of the connection status allows the user to have a current update of the panel's connection status regardless of what page is currently active. • A Lock only appears on the icon if the panel has established a connection with a currently secured target Master (*requiring a username and password*).
Connection Status:	Displays whether the panel is communicating externally, the encryption status of the communicating Master, what connection type is being used (*Ethernet or USB*), and what System the panel is a part of. This visual display of the connection status is also reflected at the upper-right of each firmware page. This allows the user to have a current visual update of the panel's connection status regardless of what page is currently active. • When a connection is established, the message displayed is either: "*Connected via Ethernet* " or "*Connected via USB* ". • If no connection can be established by the Modero panel, it will continue to try and establish a connection while displaying: "*Attempting via ...*". • The word "*Encrypted*" appears only when an encrypted connection is established with a target Master. • The panel must be rebooted before incorporating any panel communication changes and detecting any active Ethernet connections. ***The Ethernet connection is not detected until after a reboot.***
Display Timeout:	Sets the length of time the panel can remain idle before activating the sleep mode. When the device goes into sleep mode, the LCD is powered-down. • Press the UP/DN buttons to increase/decrease the time until the panel times out. Range = 0 - 240 minutes. • Use this button to set the timeout value to zero and disable the sleep mode. • Note: Display timeout values affect battery performance. Small timeout values increase the life of the battery charge. Greater timeout values may require more frequent battery charging.

Setup Page Elements (Cont.)	
Inactivity Page Flip Timeout:	Sets the number of minutes of inactivity before the panel automatically flips to a pre-selected touch panel page. When the device goes into this inactivity mode, the LCD does not power-down. • Press the UP/DN buttons to increase/decrease the time the panel can remain inactive before it flips to the preset page. Range = 0 - 240 minutes. • Use this button to set the timeout value to zero and disable the inactivity page flip mode. • The touch panel page used for the Inactivity page flip is shown within a small Inactivity Page field.
Panel Brightness:	Sets the display brightness level of the panel. • Press the UP/DN buttons to adjust the brightness level. Range = 0 - 100. • The on-screen bargraph can be dragged to adjust the Brightness level which is then reflected as a corresponding numeric value within the *Panel Brightness* field.

Information

The **Information** button provides a menu to select either the *Project Information Page* section on page 74 or the *Panel Information Page* section on page 75. Select either option to access that page.

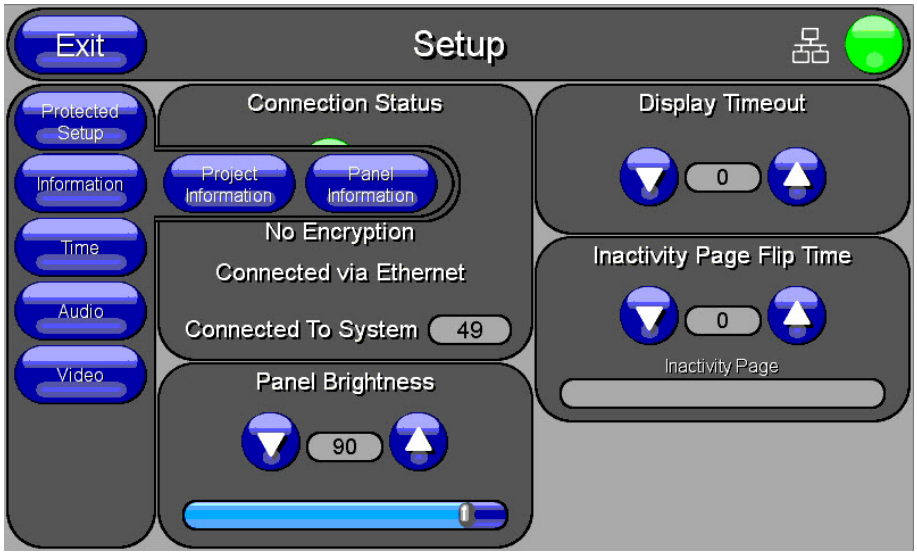


FIG. 54 Information menu

Project Information Page

The Project Information page displays the TPDesign4 (TPD4) project file properties currently loaded on the selected Modero panel (FIG. 55). Refer to the *TPDesign4 Touch Panel Program* instruction manual for more detailed program information.

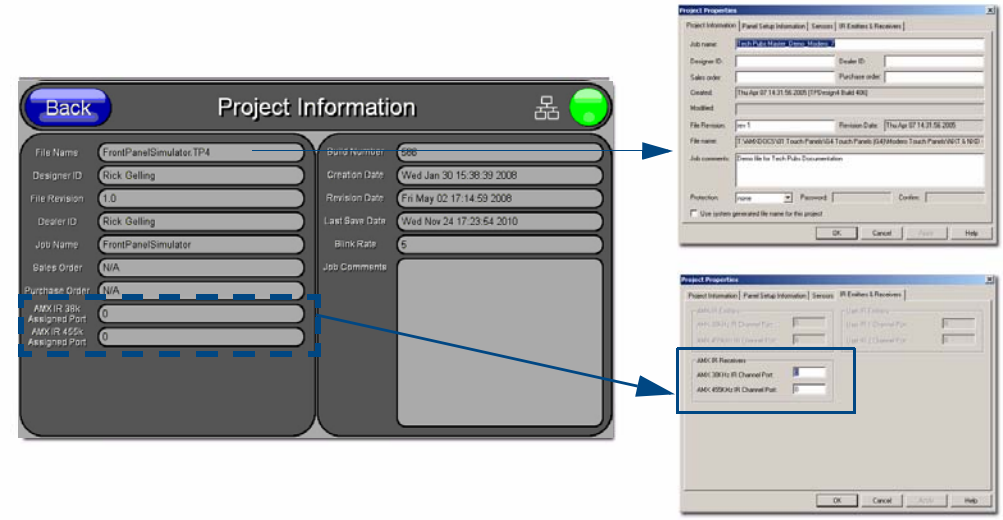


FIG. 55 Project Information page (showing the TPD4 project properties tabs)

The elements of the Project Information page are described in the table below:

Project Information Page Elements	
Back:	Returns you to the previously active touch panel page.
Connection Status icon:	This visual display of the connection status allows the user to have a current visual update of the panel's connection status regardless of what page is currently active. • A Lock only appears on the icon if the panel has established a connection with a currently secured target Master (*requiring a username and password*).
File Name:	Displays the name of the TPDesign4 project file downloaded to the panel.
Designer ID:	Displays the designer information.
File Revision:	Displays the revision number of the file.
Dealer ID:	Displays the dealer ID number (*unique to every dealer and entered in TPD4*).
Job Name:	Displays the job name.
Sales Order:	Displays the sales order information.
Purchase Order:	Displays the purchase order information.
AMX IR 38k Assigned Port:	Displays the AMX 38 kHz IR channel port used by the IR receiver on the panel. • This information is pulled by the panel from *AMX IR Receivers* section of the TPD4 Project Properties > IR Emitters & Receivers tab. • For IR reception, this is the port that reports a push on for the corresponding IR code. • IR receivers and transmitters on G4 panels share the device address number of the panel.

Project Information Page Elements (Cont.)	
AMX IR 455k Assigned Port:	Displays the AMX 455 kHz IR channel port used by the IR receiver on the panel. This information is pulled by the panel from *AMX IR Receivers* section of the TPD4 Project Properties > IR Emitters & Receivers tab. • For IR reception, this is the port that reports a push on for the corresponding IR code. • IR receivers and transmitters on G4 panels share the device address number of the panel. ***NOTE:** This feature is unavailable in NXD-700Vi panels sold after January 1, 2011.*
Build Number:	Displays the build number information of the TPD4 software used to create the project file.
Creation Date:	Displays the project creation date.
Revision Date:	Displays the last revision date for the project.
Last Save Date:	Displays the last date the project was saved.
Blink Rate:	Displays the feedback blink rate (10th of second).
Job Comments:	Displays any comments associated to the job. These comments are taken from the TPD4 project file.

Panel Information Page

The Panel Information page (FIG. 56) centers around Modero panel properties such as: resolution used, on-board memory, firmware, address/channel information, and string information.

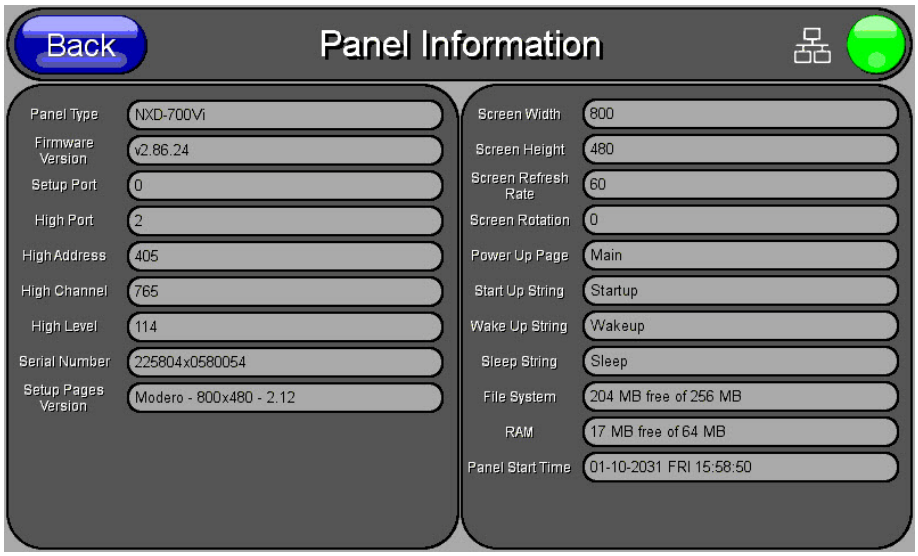


FIG. 56 Panel Information page (takes its' information from the touch panel)

The elements of the Panel Information page are described in the table below:

Panel Information Page Elements	
Back:	Returns you to the previously active touch panel page.
Connection Status icon:	This visual display of the connection status allows the user to have a current visual update of the panel's connection status regardless of what page is currently active. • A Lock only appears on the icon if the panel has established a connection with a currently secured target Master (*requiring a username and password*).
Panel Type:	Displays the model of the Modero panel being used.

Panel Information Page Elements (Cont.)	
Firmware Version:	Displays the G4 firmware version being used by the panel. • Verify you have the latest version from **www.amx.com**.
Setup Port:	Displays the setup port information/value being used by the panel.
High Port:	Displays the high port (port count) value for the panel.
High Address:	Displays the high address (address count) value for the panel.
High Channel:	Displays the high channel (channel count) value for the panel.
High Level:	Displays the high level (level count) value being used by the panel.
Serial Number:	Displays the specific serial number value assigned to the panel.
Setup Pages Version:	Displays the type and version of the Setup pages being used by the panel.
Screen Width:	Displays the pixel width being used to display the incoming video signal on the Modero panel. • Maximum available screen width on a NXD-700Vi Modero panel is 800 pixels.
Screen Height:	Displays the pixel height being used to display the incoming video signal on the Modero panel. • Maximum available screen height on a NXD-700Vi Modero panel is 480 pixels.
Screen Refresh Rate:	Displays the video refresh rate applied to the incoming video signal from the panel. *Default rate is 60.*
Screen Rotation:	Displays the degree of rotation applied to the on-screen image.
Power Up Pages:	Displays the first touch panel page assigned for display after the device is powered-up. • This information is taken from the TPD4 project file. • Most projects begin with a Main page.
Start Up String:	Displays the start-up string.
Wake Up String:	Displays the wake up string used after an activation from a timeout.
Sleep String:	Displays the sleep string used during a panel's sleep mode.
File System:	Displays the amount of Compact Flash memory available on the Modero panel.
RAM:	Displays the available RAM (or Extended Memory module) on the Modero panel.

Time & Date Settings Page

The options on the Time & Date Settings page (FIG. 57) allow you to set and adjust time and date information on the NetLinx Master. If the time and/or date on the Master is modified, all connected devices will be updated to reflect the new information.

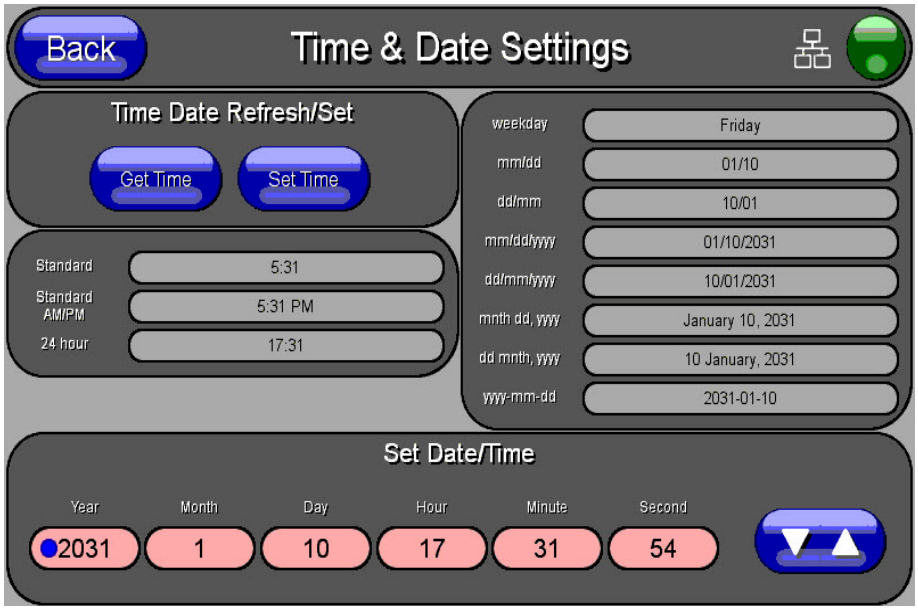


FIG. 57 Time and Date Settings page

NOTE

Touch panels do not have an on-board clock. The only way to modify a panel's time without altering the Master is via NetLinx Code.

Features on this page include:

Time & Date Settings Page	
Back:	Saves all changes and returns to the previous page.
Connection Status icon:	The icon in the upper-right corner of each Setup page provides a constant visual indication of current connection status. ***Note**: a Lock appears on the icon if the panel is connected to a secured NetLinx Master.*
Time Date Refresh/Set:	This section provides two options: • The **Get Time/Date** button retrieves Time and Date information from the Master. • The **Set Time/Date** button sets the Master to retain and save any time/date modifications made on the panel.
Time Display fields:	• These fields display the time in three formats: STANDARD, STANDARD AM/PM, and 24 HOUR.
Date Display fields:	• These fields display the calendar date information in several different formats.
Set Date/Time:	Use the UP/DN arrow buttons to adjust the Master's calendar date and time. The blue icon indicates which field is currently selected (see FIG. 57). • **Year** range = 2000 - 2037 • **Month** range = 1 - 12 • **Day** range = 1 - 31 • **Hour** = 24-hour military • **Minute** range = 0 - 59 • **Second** range = 0 - 59

Audio Settings Page

The *Audio Settings* page (accessed by pressing the **Audio** button on the *Setup* page) allows you to adjust the master volume parameters and default panel sounds on the panel. The page includes two tabs for analog (FIG. 58) and intercom (FIG. 59) sound levels.

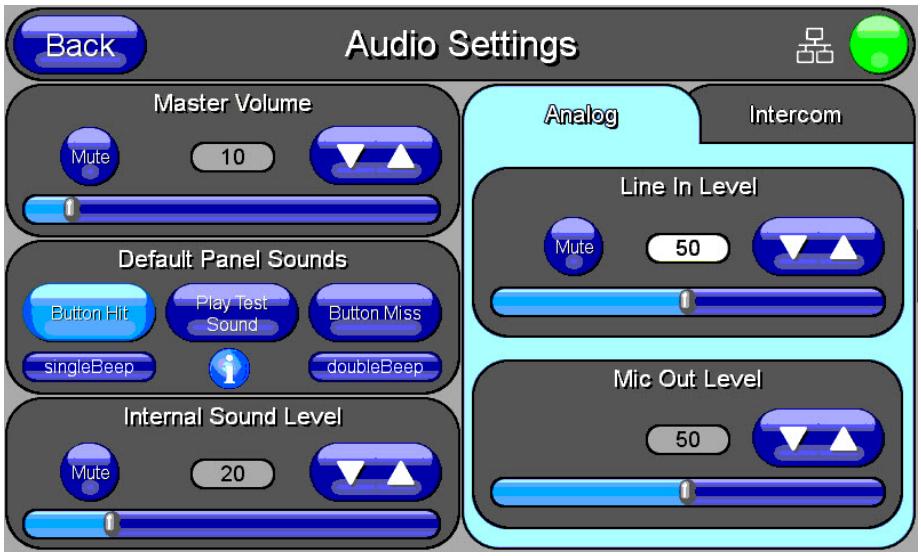


FIG. 58 Audio Settings page (Analog tab)

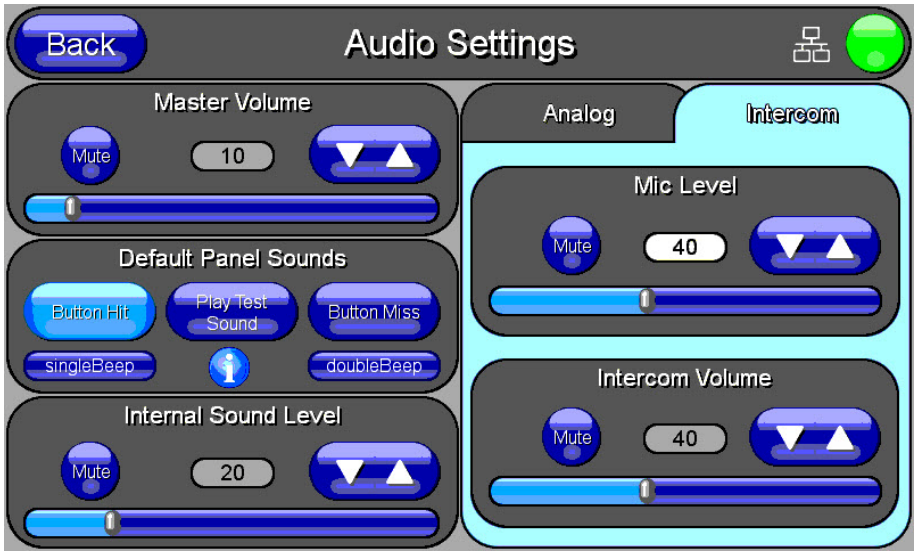


FIG. 59 Audio Settings page (Intercom tab)

The elements of the *Audio Settings* page are described in the table below:

Audio Settings Page Elements	
Back:	Saves the changes and returns you to the previously active touch panel page.
Connection Status icon:	This visual display of the connection status allows the user to have a current visual update of the panel's connection status regardless of what page is currently active. • A Lock only appears on the icon if the panel has established a connection with a currently secured target Master (*requiring a username and password*).

Audio Settings Page Elements (Cont.)	
Master Volume:	This section allows you to alter the current master volume level: • Use the **UP/DN** buttons to adjust the volume level (range = 0 - 100). • The *Master Volume* bargraph indicates the current volume level. Default = 50 • The **Mute** button toggles the Mute feature.
Default Panel Sounds:	Sets the Modero panel to play various sounds. • Activating the **Button Hit** button plays a default sound when you touch an active button. • Activating the **Button Miss** button plays a default sound when you touch a non-active button or any area outside of the active button • The **Play Test Sound** button plays a test WAV/MP3 file over the panel's internal speakers. • The **Information** button opens the *Panel Sounds Information* popup window (FIG. 60).
Digital Audio Level:	This section allows you to adjust the current sound level on the internal panel speaker: • Use the **UP/DN** buttons to adjust the volume output on the internal speakers (range = 0 - 100). • The *Internal Sound Level* bargraph indicates the current sound level. Default = 50 • The **Mute** button mutes the volume.
Analog:	
Line In Level:	Allows you to adjust the current Line-In volume level (being received from the communicating breakout box). • Use the UP/DN buttons to adjust the Line-In volume level (range = 0 - 100). • The Line-In Level bargraph indicates the current Line-In level. • The **Mute** button mutes the Line-In volume.
Mic Out Level:	Allows you to adjust the current Microphone volume level (being received from the communicating breakout box). • Use the UP/DN buttons to adjust the Microphone volume level (range = 0 - 100). • The Mic Out Level bargraph indicates the current Mic Out level.
Intercom:	
Mic Level:	Adjusts the volume level on the panel's microphone • Use the UP/DN buttons to adjust the microphone level (range = 0 - 100) • The Mic Out Level bargraph indicates the current Mic Out level Default = 40
Intercom Volume:	Sets the volume level for intercom calls • Use the UP/DN buttons to adjust the Line-In volume level (range = 0 - 100) • The Line-In Level bargraph indicates the current Line-In level • The **Mute** button mutes the Line-In volume Default = 40

Environmental acoustics, personal voice level and ambient noise are all deciding factors when setting your mic, intercom and panel sound levels. Consider your environment when adjusting intercom and sound levels and use caution so as not to damage the speaker.

Panel Sounds Information Popup Window

Clicking the **Information** button in the *Default Panel Sounds* section opens the *Panel Sounds Information* popup window (FIG. 60). Click the **Close** button to return to the *Audio Settings* page.

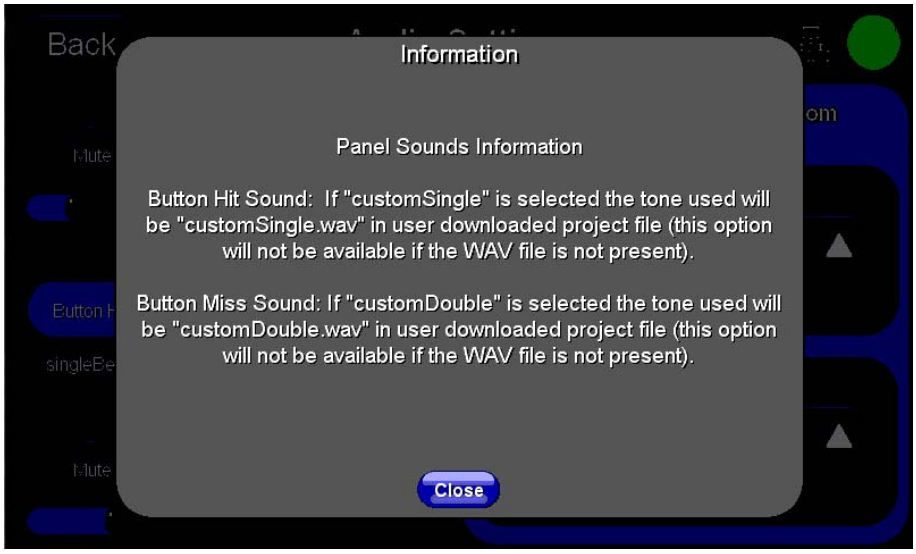


FIG. 60 Panel Sounds Information popup window

Supported sampling rates for WAV

The following is a listing of supported sampling rates associated for WAV files played on NXD-700Vi panels. Some WAV files currently played on Modero's may not work on these panels. The supported sampling rates for WAV files are:

Supported WAV Sampling Rates	
• 48000 Hz	• 16000 Hz
• 44100 Hz	• 12000 Hz
• 32000 Hz	• 11025 Hz
• 24000 Hz	• 8000 Hz
• 22050 Hz	

Video Settings Page

The Video Settings page (FIG. 61) (accessed by pressing the **Video** button on the *Setup* page) sets the Video properties of the incoming video signal from an NXA-AVB/ETHERNET Breakout Box.

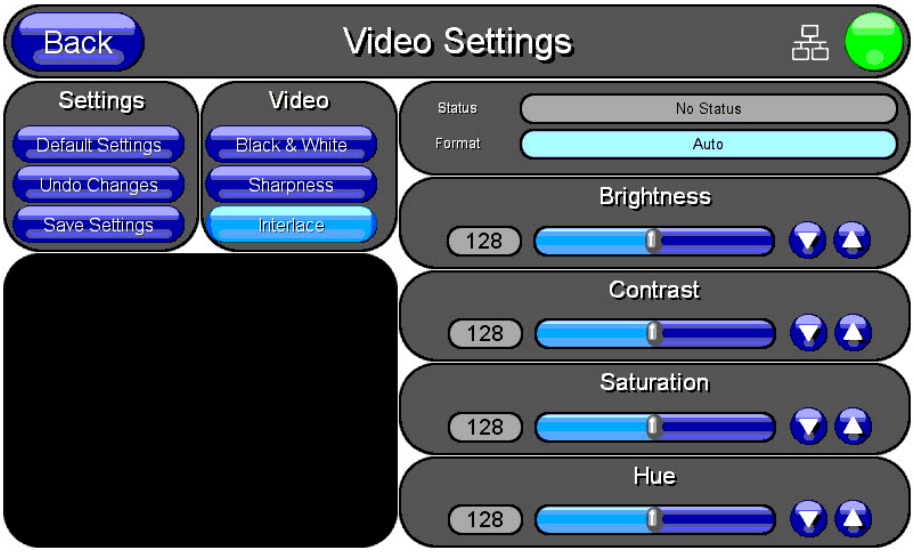


FIG. 61 Video Settings page (showing default values)

The elements of the *Video Settings* page are described in the table below:

Video Settings Page Elements	
Back:	Saves the changes and returns you to the previously active touch panel page.
Connection Status icon:	This visual display of the connection status allows the user to have a current visual update of the panel's connection status regardless of what page is currently active. • A Lock only appears on the icon if the panel has established a connection with a currently secured target Master (*requiring a username and password*).
Settings:	• The **Default Settings** button sets the video settings to their default values (indicated in this table). • The **Undo Changes** button disregards any changes made on the page since the last settings were saved. • The **Save Settings** button saves any changes made to this page.
Video:	• The **Black & White** button toggles the Black & White display mode. Default = Off. • The **Sharpness** button toggles the Interpolate (Sharpness) feature. Default = Off. • The **Interlace** button toggles the Interlacing feature. Default = On.
Status:	Displays whether or not a video-sync signal is detected.
Format:	Allows you to press this blue field and cycle through a choice of available video formats (**NTSC**, **PAL**, **SECAM**, or **Auto detect**). • Default = Auto.
Brightness:	Use the UP/DN buttons to alter the brightness level of the incoming signal. • Range = 0 - 255, default = 128.
Contrast:	Use the UP/DN buttons to alter the contrast level of the incoming signal. • Range = 0 - 255, default = 128.
Saturation:	Use the UP/DN buttons to alter the color saturation level of the incoming signal. • Range = 0 - 255, default = 128.

Video Settings Page Elements (Cont.)	
Hue:	Use the UP/DN buttons to alter the hue level of the incoming signal. • Range = 0 - 255, default = 128.

Protected Setup Navigation Buttons

The Protected Setup Navigation Buttons (FIG. 62) appear on the left of the panel screen when the *Protected Setup* page is currently active.

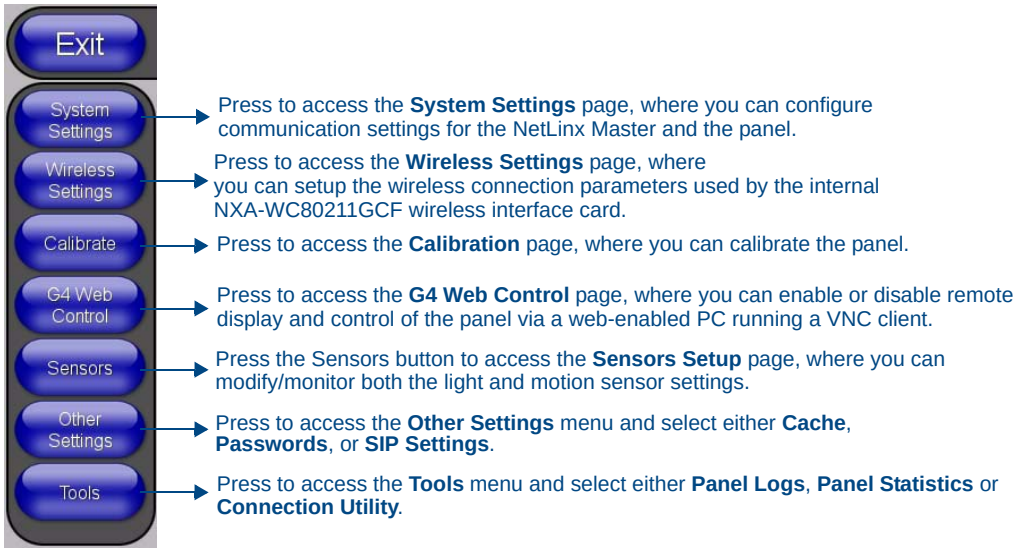


FIG. 62 Protected Setup Navigation Buttons

Protected Setup Page

The Protected Setup page (FIG. 63) centers around the properties used by the panel to properly communicate with the NetLinx Master. Enter the factory default password (***1988***) into the password keypad to access this page for the first time.

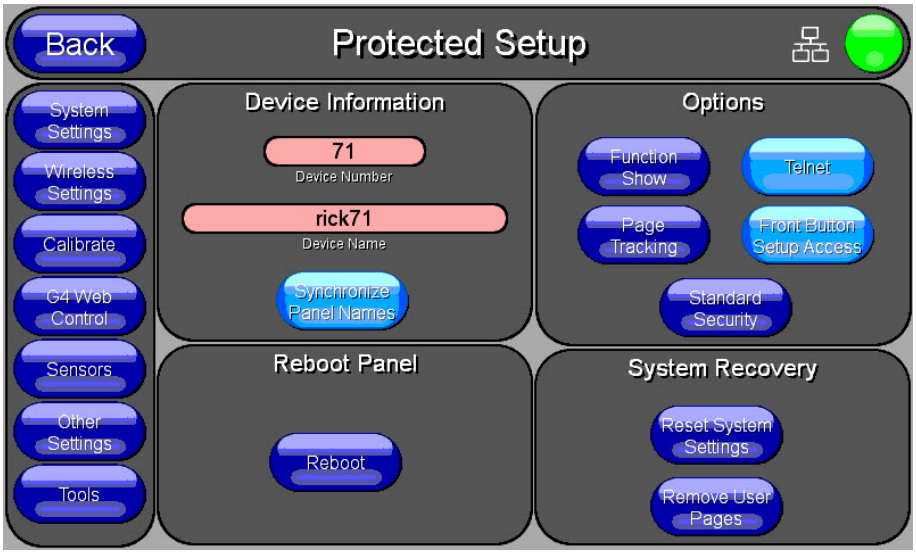


FIG. 63 Protected Setup page - showing default values

The elements of the *Protected Setup* page are described in the table below:

Protected Setup Page Elements	
Back:	Saves the changes and returns you to the previously active touch panel page.
Connection Status icon:	This visual display of the connection status allows the user to have a current visual update of the panel's connection status regardless of what page is currently active. • A Lock only appears on the icon if the panel has established a connection with a currently secured target Master (*requiring a username and password*).
Device Information:	Opens keypads used to set and display the current device number and device name. • Press the **Synchronize Panel Names** button to allow of the Device Name and the G4 Web Control Name (FIG. 65).
Options:	Allows you to select various touch panel features: • The **Function Show** button enables the display of the channel port and channel code in the top left corner of the button, the level port and level code in the bottom left corner, and the address port and address code in the bottom right corner (see FIG. 66 for an example of the function locations). • Use the **Page Tracking** button to toggle page tracking. When enabled, the touch panel sends page data back to the NetLinx Master, or vice versa depending on the touch panel settings. • Use the **Telnet** button to enable or disable the telnet server on the panel. This feature focuses on direct telnet communication to the panel. • Use the **Front Button Setup Access** button to activate the grey Front Setup Access button (located below the LCD) to access the firmware pages. - Default condition is On. - Press and hold this grey button for **3 seconds** to access the *Setup* page. - Press and hold this grey button for **6 seconds** to access the *Calibration* page.
Reboot Panel:	Pressing this button causes the panel to restart after saving any changes.

Protected Setup Page Elements (Cont.)	
System Recovery:	Allows you to either reset the touch panel to factory default settings and/or wipe out all existing touch panel pages: • The **Reset System Settings** button allows a user to wipe out all current configuration parameters on the touch panel (such as IP Addresses, Device Number assignments, Passwords, and other presets). - Pressing this button launches a Confirmation dialog (FIG. 64) which asks you to confirm your selection. - This dialog is configured with a delay timer that does not enable the YES button for 5 seconds. This delay provides an additional amount of time for the user to confirm their decision. • The **Remove User Pages** button allows you remove all current TPD4 touch panel pages currently on the panel (*including the pre-installed AMX Demo pages*). - Pressing this button launches a Confirmation dialog (FIG. 64) which asks you to confirm your selection. - This dialog is configured with a delay timer that does not enable the YES button for 5 seconds. This delay provides an additional amount of time for the user to confirm their decision.

FIG. 64 Protected Setup page-System Recovery confirmation dialog

FIG. 65 Protected Setup page - Device Name change confirmation dialog

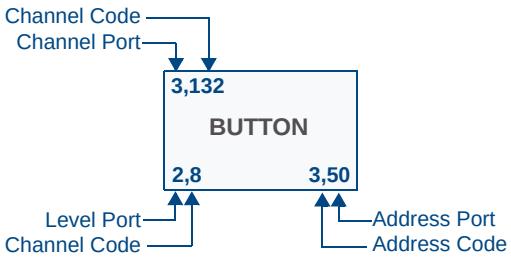


FIG. 66 Button/slider Function Show example

System Settings Page

The System Settings page (FIG. 67) sets the Secondary DNS Address information with its corresponding IP communication parameters, NetLinx Master communication settings, and reads the device number assigned to the Modero panel.

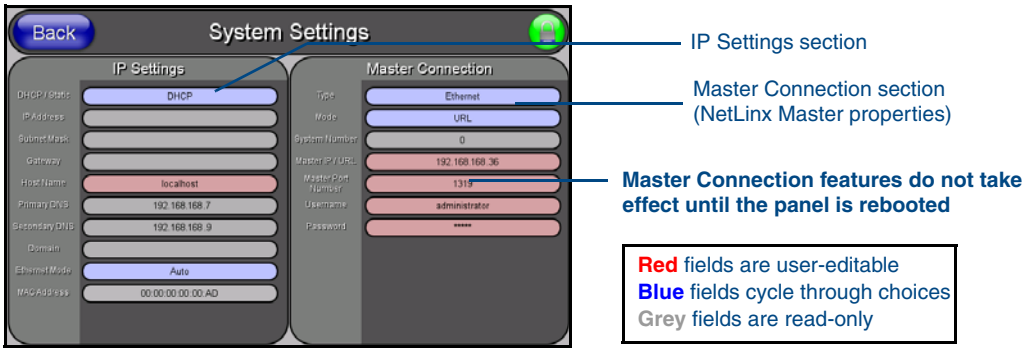


FIG. 67 System Settings page showing default values (reads and assigns values to the panel and Master)

The elements of the System Settings page are described in the table below:

System Settings Page Elements	
Back:	Saves the changes and returns you to the previously active touch panel page.
Connection Status icon:	This visual display of the connection status allows the user to have a current visual update of the panel's connection status regardless of what page is currently active. • A Lock only appears on the icon if the panel has established a connection with a currently secured target Master (*requiring a username and password*).

System Settings Page Elements (Cont.)	
IP Settings:	Sets the IP communication values for the panel and contains:
DHCP/Static	Sets the panel to either DHCP or Static communication modes. • *DHCP (Dynamic Host Configuration Protocol)* assigns IP Addresses from client stations logging onto a TCP/IP network via a DHCP server. • *Static IP* is a permanent IP Address that is assigned to a node in a TCP/IP network.
IP Address	Sets the secondary IP Address assigned to the panel.
Subnet Mask	Sets a subnetwork address to the panel. • *Subnetwork mask* is the technique used by the IP protocol to filter messages into a particular network segment (Subnet).
Gateway	Sets a gateway value to the panel. • *Gateway* is a computer that either performs protocol conversion between different types of networks/applications or acts as a go-between two or more networks that use the same protocols.
Host Name	Sets the host name of the panel.
Primary DNS	Sets the address of the primary DNS server used for host name lookups. • *DNS (Domain Name System)* is software that lets users locate computers on a local network or the Internet (TCP/IP network) by host and domain. The DNS server maintains a database of host names for its' domain and their corresponding IP Addresses.
Secondary DNS	Sets a secondary DNS value to the panel.
Domain	Sets the unique name on the Internet to the panel for DNS look-up. • The panel belongs to the DNS domain.
Ethernet Mode	Sets the speed of the Ethernet connection to the panel. • Choices are: **Auto**, **10 Half Duplex**, **10 Full Duplex**, **100 Half Duplex,** or **100 Full Duplex.**
MAC Address	Displays a read-only field that is factory set by AMX for the built-in Ethernet interface.
Master Connection:	Sets the NetLinx Master communication values:
Type	Sets the NetLinx Master to communicate with the panel via either USB or Ethernet. This is based on the cable connection from the rear. ***ICSNet is not a supported option on this panel.*** • *Ethernet* is a CAT-5 cable (10/100Base T terminated in an RJ-45 connector) used to network computers together and is used in most LAN (local area networks). This description is also used to refer to both wired and wireless communication. • *USB* option cannot be used on Modero panels which are not equipped with a rear USB port.
Mode	Cycles between the different connection modes (URL, Listen, and Auto) ***(ETHERNET Only - disabled when USB is selected)*** • **URL** - In this mode, enter the IP/URL, Master Port Number, and username/password (if used) on the Master. - The System Number field is read-only because the panel obtains this information from the communicating Master. • **Listen** - In this mode, add the Modero panel address into the URL List in NetLinx Studio and set the connection mode to Listen. This mode allows the Modero touch panel to "listen" for the Master's communication signals. - The System Number and Master IP/URL fields are red-only. • **Auto** - In this mode, enter the System Number and a username/password (if applicable). This mode is used when both the panel and the NetLinx Master are on the same Subnet and the Master has its UDP feature enabled. - Master IP/URL field is read-only.

System Settings Page Elements (Cont.)	
Master Connection (Cont.):	
System Number	Allows you to enter a system number. Default value is 0 (zero). ***(ETHERNET Only - disabled when USB is selected)***
Master IP/URL	Sets the Master IP or URL of the NetLinx Master. ***(ETHERNET Only - disabled when USB is selected)***
Master Port Number	Allows you to enter the port number used with the NetLinx Master. • Default value is 1319. ***(ETHERNET Only - disabled when USB is selected)***
Username/Password	If the target Master has been previously secured, enter the alpha-numeric string (into each field) assigned to a pre-configured user profile on the Master. This profile should have the pre-defined level of access/configuration rights.

Refer to the *Step 3: Choose a Master Connection Mode* section on page 52 for more detailed information on using the System Settings page.

Wireless Settings Page

Use the options on the Wireless Settings page (FIG. 68) to configure communication settings for the wireless CF card (802.11g), and read the device number assigned to the panel.

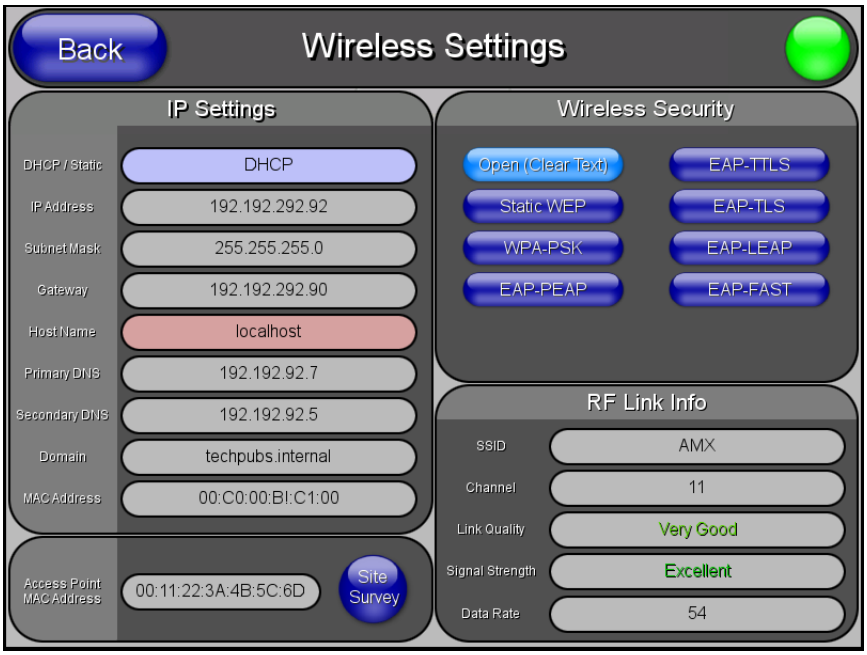


FIG. 68 Wireless Settings page (reads from and assigns values to the WAP)

Features on this page include:

Wireless Settings Page	
Back:	Saves all changes and returns to the previous page.
Connection Status icon:	The icon in the upper-right corner of each Setup page provides a constant visual indication of current connection status. ***Note**: a Lock appears on the icon if the panel is connected to a secured NetLinx Master.*

Wireless Settings Page (Cont.)	
IP Settings:	Sets the IP communication values for the panel:
DHCP/STATIC	Sets the panel to either DHCP or Static communication modes. • *DHCP* - a temporary IP Addresses is assigned to the panel by a DHCP server. • *Static IP* is a permanent IP Address assigned to the panel. If Static IP is selected, the other *IP Settings* fields are enabled (below).
IP Address	Enter the secondary IP address for this panel.
Subnet Mask	Enter the subnetwork address for this panel.
Gateway	Enter the gateway address for this panel.
Host Name	Enter the host name for this panel.
Primary DNS	Enter the address of the primary DNS server used by this panel for host name lookups.
Secondary DNS	Enter the secondary DNS address for this panel.
Domain	Enter a unique name to the panel for DNS look-up.
MAC Address	This unique address identifies the wireless Ethernet card in the panel (read-only).
Access Point MAC Address:	This unique address identifies the Wireless Access Point (WAP) used by this panel for wireless communication (read-only). • **Site Survey** button: Launches the Site Survey page. The options on this page allow you to detect ("sniff-out") all WAPs transmitting within range of the panel's *NXA-WC80211GCF* Wi-Fi card. Data displayed on the Site Survey page is categorized by: - **Network Name (SSID**) - WAP names - **Channel (RF)** - channels currently being used by the WAP - **Security Type** - security protocol enabled on the WAP, if detectable - **Signal Strength** - None, Poor, Fair, Good, Very Good, and Excellent - **MAC Address** - Unique identification of the transmitting Access Point • Refer to the *Using the Site Survey tool* section on page 44 for more detailed information on the SIte Survey page. • When communicating with a NXA- WAP200G, enter the MAC Address (**BSSID**) of the target WAP as the Access Point MAC Address. Refer to the ***WAP200G*** *Instruction Manual* for more information.
Wireless Security:	Sets the wireless security method to be used by the panel to connect to the network. Selecting any of the connection method buttons invokes the relevant configuration page, with options that allow you to define parameters specific to the selected method of connection. • Refer to the following *Wireless Security Page* section on page 91 for further details on these security options.
Open (Clear Text)	This button opens the Open (Clear Text) Settings page (FIG. 69 on page 92). "Open" security does not utilize any encryption methodology, but requires an SSID (alpha-numeric) entry. This entry must match the Network Name (SSID) entry of the target WAP so the panel knows what device it is using to communicate with the network. • Refer to the following *Wireless Security Page* section on page 91 for further details on these security options.
Static WEP	This button opens the Static WEP Settings page (FIG. 70 on page 93). "Static WEP" security requires that both a target WAP be identified and an encryption method be implemented prior to establishing communication. • Refer to the *Wireless Security Page* section on page 91 for further details on these security options.

Wireless Settings Page (Cont.)	
Wireless Security (Cont.):	
WPA-PSK	This button opens the WPA-PSK Settings page (FIG. 71 on page 95). "WPA-PSK" security is designed for environments where is it desirable to use WPA or WPA2, but an *802.1x authentication server is not available*. PSK connections are more secure than WEP and are simpler to configure since they implement dynamic keys but share a key between the WAP and the panel (client). • Refer to the *Wireless Security Page* section on page 91 for details.
EAP-PEAP	This button opens the EAP-PEAP Settings page (FIG. 75 on page 100). "EAP-PEAP" security is designed for wireless environments where it is necessary to securely transmit data over a wireless network. • Refer to the *Wireless Security Page* section on page 91 for details. • For information on uploading a certificate file, refer to the *AMX Certificate Upload Utility* section on page 203.
EAP-TTLS	This button opens the EAP-TTLS Settings page (FIG. 76 on page 102). "EAP-TTLS" security is designed for wireless environments where it is necessary to first have a Radius server directly validate the identity of the client (panel) before allowing it access to the network. • Refer to the *Wireless Security Page* section on page 91 for details. • For information on uploading a certificate file, refer to the *AMX Certificate Upload Utility* section on page 203.
EAP-TLS	This button opens the EAP-TLS Settings page (FIG. 77 on page 104). "EAP-TLS" security is designed for wireless environments where it is necessary to securely transmit data over a wireless network by adding an additional level of security protocol via the use of a private key. • Refer to the *Wireless Security Page* section on page 91 for details. • For information on uploading a certificate file, refer to the *AMX Certificate Upload Utility* section on page 203.
EAP-LEAP	This button opens the EAP-LEAP Settings page (FIG. 72 on page 97). "EAP-LEAP" security is designed for wireless environments where it is not required to have both a client or server certificate validation scheme in place, yet necessary to securely transmit data over a wireless network. • Refer to the *Wireless Security Page* section on page 91 for details.
EAP-FAST	This button opens the EAP-FAST Settings page (FIG. 74 on page 99). "EAP-FAST" security is designed for wireless environments where security and ease of setup are equally desirable. • Refer to the *Wireless Security Page* section on page 91 for details.
Site Survey:	The Site Survey tool allows you to detect and view detailed information on all WAPs within the panel's communication area. Using this tool, you can select a WAP to connect to. • Refer to the *Using the Site Survey tool* section on page 44 for information on using this tool.
RF Link Info:	These options set communication values for the wireless interface card:
SSID	Displays the currently used SSID of the target WAP.
Channel	The RF channel being used for connection to the WAP (*read -only*).

Wireless Settings Page (Cont.)	
RF Link Info (Cont.):	
Link Quality	Displays the quality of the link from the wireless NIC to the Wireless Access Point (direct sequence spread spectrum) in real time (*None*, *Poor*, *Fair*, *Good*, *Very Good*, and *Excellent*). • Even when link quality is at its lowest you still have a connection, and the ability to transmit and receive data, even if at lower speeds. ***Note:*** *"Link Quality" and "Signal Strength" are applicable to RF connections only. It is possible to have an RF signal to a WAP, but be unable to communicate with it because of either incorrect IP or encryption settings.*
Signal Strength	This indicator displays a description of the signal strength from the Wireless Access Point connection in real time (*None*, *Poor*, *Fair*, *Good*, *Very Good*, and *Excellent*). SNR (Signal Noise Ratio) is a measure of the relative strength of a wireless RF connection. Given this value and the link quality above, you can determine the noise level component of the SNR. For example, if signal strength is high but the link quality is low, then the cause of the link degradation is noise. However, if signal strength is low and link quality is low the cause would simply be signal strength.
Data Rate	The data rate (in Mbps) at which the panel is currently communicating with the target WAP. ***Note****: Data rates for 802.11b communication are: 1, 2, 5.5, and 11 Mbps.*

Secondary Connection Page

The Secondary Connection page sets the communication information for an installed wireless interface card. The NXD-CV5 Touch panel is not enabled for wireless communication and therefore, this page is not user-editable.

Wireless Security Page

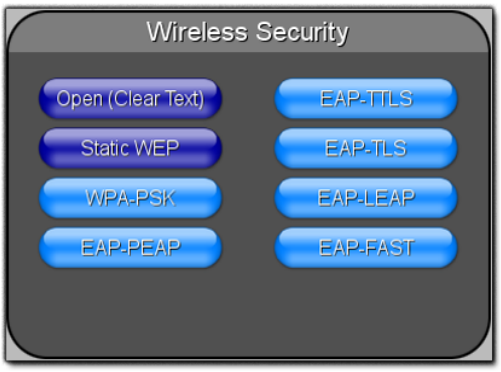
The options on the Wireless Security page allow you to select from the wireless security methods supported by the NXA-WC80211GCF Wi-Fi card. These security methods incorporate *WPA*, *WPA2*, and *EAP* technology (some of which require the upload of unique certificate files to a target panel).

Refer to the *Appendix B - Wireless Technology* section on page 197 for more further information.

Some encryption and security features may/may not be supported depending on the type of wireless card being used:

Wireless Security Support	
802.11g Wi-Fi CF card:	• Open (Clear Text) • Static WEP (64-bit and 128-bit key lengths) • WPA-PSK • EAP security (with and without certificates) • WAP SIte Survey

Refer to the *Configuring a Wireless Network Access* section on page 43 for more information on configuring the panel for wireless network access using the various security options.



802.11g wireless card

Wireless Security pages (each Wi Fi card supports different security features)

Open (Clear Text) Settings

Press the **Open (Clear Text)** button to open the Open (Clear Text) Settings page (FIG. 69).

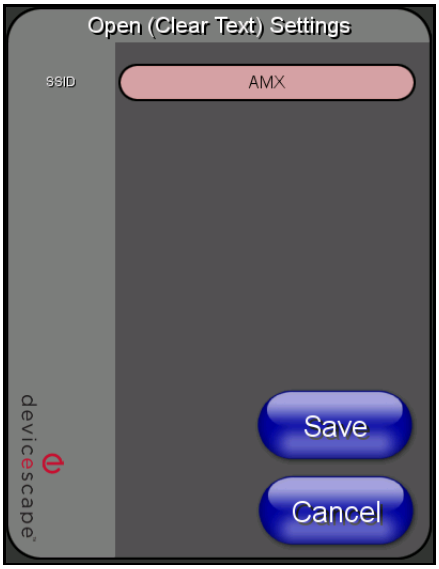


FIG. 69 Wireless Settings page - Open (Clear Text) Settings

Open security does not utilize any encryption methodology, but requires an SSID (alpha-numeric) entry. This entry must match the Network Name (SSID) entry of the target WAP so the panel knows what device it is using to communicate with the network.

Open (Clear Text) Settings	
SSID (Service Set Identifier):	Opens an on-screen keyboard to enter the SSID name used on the target WAP. The SSID is a unique name used by the WAP, and is assigned to all panels on that network. An SSID is required by the WAP before the panel is permitted to join the network. • The SSID is case sensitive and must not exceed 32 characters. • Make sure this setting is the same for all points in your wireless network. • NXA-WAP200Gs use **AMX** as their default SSID. • If this field is left blank, the panel will attempt to connect to the first available WAP.
Save/Cancel:	• **Save** - store the new security information, apply changes, and return to the previous page. • **Cancel** - discard changes and return to the previous page.

- Refer to the *Configuring a Wireless Network Access* section on page 43 for further details on these security options.
- Refer to the *Using the Site Survey tool* section on page 44.

Static WEP Settings

Press the **Static WEP** button to open the Static WEP Settings page (FIG. 70).

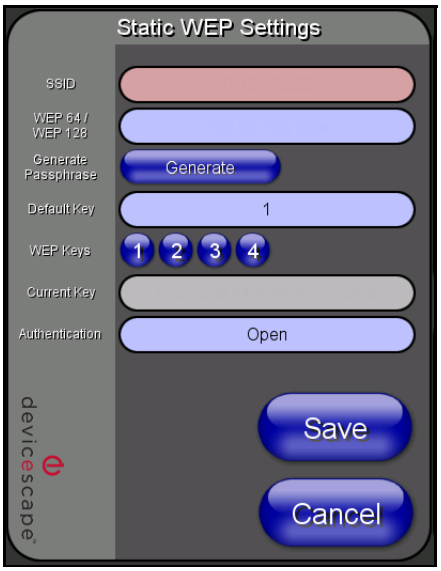


FIG. 70 Wireless Settings page - Static WEP Settings

Static WEP security requires that both a target WAP be identified and an encryption method be implemented prior to establishing communication. In addition to providing both Open and Shared Authentication capabilities, this page also supports Hexadecimal and ASCII keys.

Static WEP Settings	
SSID (Service Set Identifier):	Opens an on-screen keyboard to enter the SSID name used on the target WAP. The SSID is a unique name used by the WAP, and is assigned to all panels on that network. An SSID is required by the WAP before the panel is permitted to join the network. • The SSID is case sensitive and must not exceed 32 characters. • Make sure this setting is the same for all points in your wireless network. • NXA-WAP200Gs use **AMX** as their default SSID. • If this field is left blank, the panel will attempt to connect to the first available WAP.
WEP 64 / WEP 128:	Cycles through the available encryption options: *64 or 128 Bit Key Size*. "WEP" (Wired Equivalent Privacy) is an 802.11 security protocol designed to provide wireless security equivalent to wired networks. • **WEP64** enables WEP encryption using a 64 Bit Key Size. All packets are transmitted with their contents encrypted using the Default WEP Key. • **WEP128** enables WEP encryption using a 128 Bit Key Size. All packets are transmitted with their contents encrypted using the Default WEP Key. • If the key is not the correct size, the system will resize it to match the number of bits required for the WEP encryption mode selected.
Generate (Passphrase):	This button displays an on-screen keyboard which allows you to enter a passphrase. The panel then automatically generates four WEP keys (compatible only with Modero panels). Enter these WEP keys into the target WAP. When working with multiple panels, WEP Keys must be entered into the WAP for each panel. • All Modero panels use the same code key generator. Therefore, this Passphrase generates identical keys on any Modero panel. • The Passphrase generator is case sensitive. ***Note**: This Key generator is unique to Modero panels and does not generate the same keys as non-AMX wireless devices. For example, a Current Key string generated anywhere else will not match those created on Modero panels.*
Default Key:	Cycles through the four available WEP key identifiers to select a WEP key to use. As the Default Key value is altered (through selection) the corresponding "Current Key" is displayed. Each Current Key corresponds to a WEP key. This feature is useful for accessing different networks without having to re-enter that networks' WEP key. It is also sometimes used to set up a rotating key schedule to provide an extra layer of security.
WEP Keys:	This feature provides another level of security by selecting up to four WEP Keys. Push any of the four buttons to open an on-screen keyboard. Both ASCII and HEX keys are supported. Up to four keys can be configured for both. • An ASCII key utilizes either 5 or 13 ASCII characters • A HEX key utilizes either 10 or 26 Hexidecimal characters Press **Done** to accept any changes and save the new value. ***Note**: A 64-bit key will be 10 characters in length while a 128-bit key will be 26 characters in length. The length of the key entered determines the level of WEP encryption employed (64 or 128-bit). 128-bit keys may be used if supported by the internal wireless card.*

Static WEP Settings (Cont.)	
Current Key:	Displays the current WEP key in use. • When working with a single panel and a single WAP, it is recommended that you manually enter the *Current Key* from the WAP into the selected WEP Key. • When working with a single WAP and multiple panels, it is recommended that you generate a Current Key using the same passphrase on all panels and then enter the panel-produced WEP key manually into the Wireless Access Point. • Keys may also be examined by touching the key buttons and noting the keyboard initialization text. • Use the on-screen keyboard's **Clear** button to erase stored key information.
Authentication:	Toggles between the two authentication modes: *Open + WEP* (broadcast publicly) or *Shared + WEP* (encrypted). • An *Open + WEP* network allows connections from any client without authentication. • A *Shared + WEP* network requires the client to submit a key which is shared by the network WAP before it is given permission to associate with the network. In this case the key is the same as the WEP encryption key. In either case, if WEP encryption has been enabled, the client will still require the WEP key to encrypt and decrypt packets in order to communicate with the network.
Save/Cancel:	• **Save** - store the new security information, apply changes, and return to the previous page. • **Cancel** - discard changes and return to the previous page.

- Refer to the *Configuring a Wireless Network Access* section on page 43 for further details on these security options.
- Refer to the *Using the Site Survey tool* section on page 44 for more information on using this feature.

WPA-PSK Settings

Press the **Static WEP** button to opens the Static WEP Settings dialog (FIG. 71).

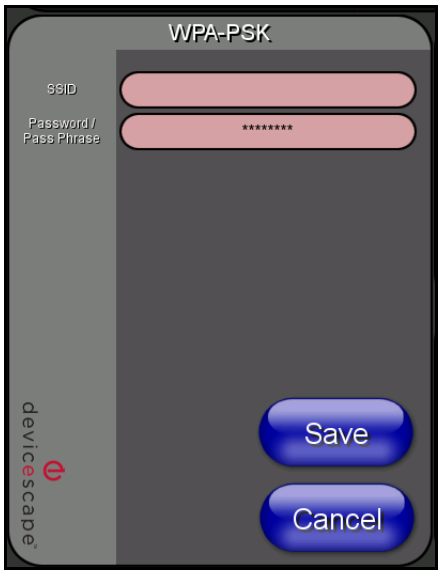


FIG. 71 Wireless Settings page - WPA-PSK Settings

WPA-PSK security is designed for environments where is it desirable to use WPA or WPA2, but an 802.1x authentication server is not available. PSK connections are more secure than WEP and are simpler to configure since they implement dynamic keys but share a key between the WAP and the panel (client).

Using WPA-PSK, the encryption on the WAP could either be WPA or WPA2. The firmware in the panel will automatically connect to the WAP using the correct encryption. The WPA encryption type is configured on the WAP, not in the firmware.

WAPs do not display “WPA” or “WPA2” on their configuration screens:

- *WPA* is normally displayed as *TKIP*.
- *WPA2* is normally displayed as *AES CCMP*.

The following fields are required: *SSID* and *Password/Pass Phrase*.

- Enter the SSID of the WAP.
- Enter a pass phrase with a minimum of 8 characters and a maximum of 63.
- The exact same pass phrase (including capitalization) must be entered in the access point.

WPA-PSK Settings	
SSID (Service Set Identifier):	Opens an on-screen keyboard to enter the SSID name used on the target WAP. The SSID is a unique name used by the WAP, and is assigned to all panels on that network. An SSID is required by the WAP before the panel is permitted to join the network. • The SSID is case sensitive and must not exceed 32 characters. • Make sure this setting is the same for all points in your wireless network. • NXA-WAP200Gs use **AMX** as their default SSID. • If this field is left blank, the panel will attempt to connect to the first available WAP.
Password/Pass Phrase:	Opens an on-screen keyboard to enter a passphrase (password). • This alpha-numeric string must use a minimum of 8 characters and a maximum of 63. • The exact pass phrase string (including capitalization) must be entered on the target WAP.
Save/Cancel:	• **Save** - store the new security information, apply changes, and return to the previous page. • **Cancel** - discard changes and return to the previous page.

- Refer to the *Configuring a Wireless Network Access* section on page 43 for details on these security options.
- Refer to the *Using the Site Survey tool* section on page 44 for more information on using this tool.

EAP-LEAP Settings

Press the **EAP-LEAP** button to open the EAP-LEAP Settings page (FIG. 72).

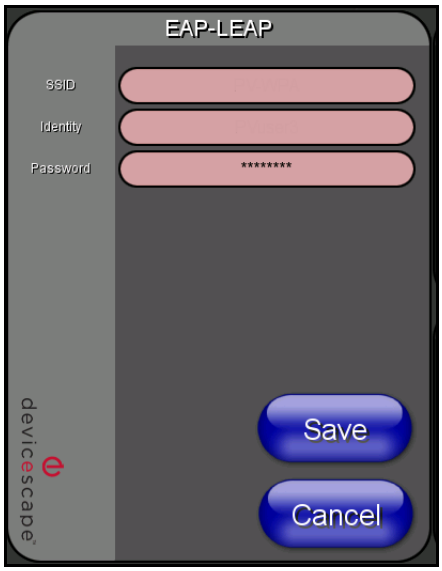


FIG. 72 Wireless Settings page - EAP-LEAP Settings

EAP (Extensible Authentication Protocol) is an Enterprise authentication protocol that can be used in both wired and wireless network environments. EAP requires the use of an 802.1x Authentication Server, also known as a Radius server. The configuration fields described below take variable length strings as inputs. An on-screen keyboard is opened when these fields are selected.

LEAP (Lightweight Extensible Authentication Protocol) was developed to transmit authentication information securely in a wireless network environment.

NOTE

LEAP does not use client (panel) or server (RADIUS) certificates and is therefore one of the least secure EAP security methods but can be utilized successfully by implementing sufficiently complex passwords.

EAP-LEAP security is designed for wireless environments where it is not required to have a client or server certificate validation scheme in place, yet necessary to transmit data securely over a wireless network.

EAP-LEAP Settings	
SSID (Service Set Identifier):	Opens an on-screen keyboard to enter the SSID name used on the target WAP. The SSID is a unique name used by the WAP, and is assigned to all panels on that network. An SSID is required by the WAP before the panel is permitted to join the network. • The SSID is case sensitive and must not exceed 32 characters. • Make sure this setting is the same for all points in your wireless network. • NXA-WAP200Gs use **AMX** as their default SSID. • With EAP security, the SSID of the WAP *must* be entered. If it is left blank, the panel will try to connect to the first access point detected that supports EAP. However, a successful connection is not guaranteed because the detected WAP may be connected to a RADIUS server, which may not support this EAP type and/or have the proper user identities configured.

EAP-LEAP Settings (Cont.)	
Identity:	Opens an on-screen keyboard. Enter an EAP Identity string (used by the panel to identify itself to an Authentication (RADIUS) Server). ***Note**: This information is similar to a username used to login to a secured server or workstation. This works in tandem with the Password string which is similar to the password entered to gain access to a secured workstation. Typically, this is in the form of a username such as: jdoe@amx.com.*
Password:	Opens an on-screen keyboard. Enter the network password string specified for the user entered within the *Identity* field (used by the panel to identify itself to an Authentication (RADIUS) Server) ***Note**: This information is similar to the password entered to gain access to a secured workstation.*
Save/Cancel:	• **Save** - store the new security information, apply changes, and return to the previous page. • **Cancel** - discard changes and return to the previous page.

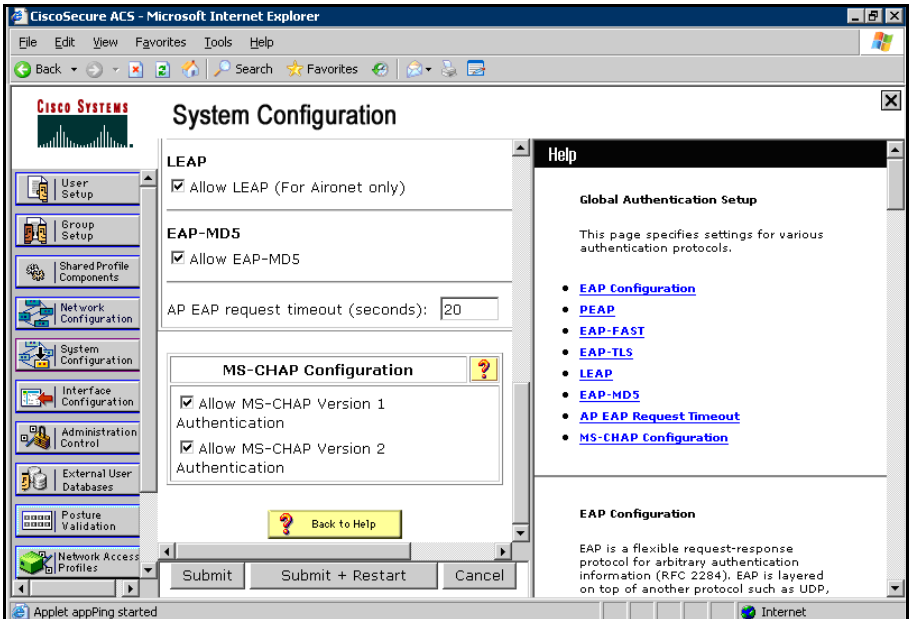


FIG. 73 EAP-LEAP sample Cisco System Security page

- Refer to the *EAP Authentication* section on page 201 for further details on these security options.
- Refer to FIG. 73 for an example of what a typical EAP-LEAP system configuration page would like.

EAP-FAST Settings

Press the **EAP-FAST** button to open the EAP-FAST Settings dialog (FIG. 74).

EAP-FAST (Flexible Authentication via Secure Tunneling) security was designed for wireless environments where security and ease of setup are equally desirable. EAP-FAST uses a certificate file, however it can be configured to download the certificate automatically the first time the panel attempts to authenticate itself. Automatic certificate downloading is convenient but slightly less secure, since its the certificate is transferred wirelessly and could theoretically be “sniffed-out”.

- Refer to the *EAP Authentication* section on page 201 for further details on these security options.
- Refer to the *Using the Site Survey tool* section on page 44 for more information on using this feature.

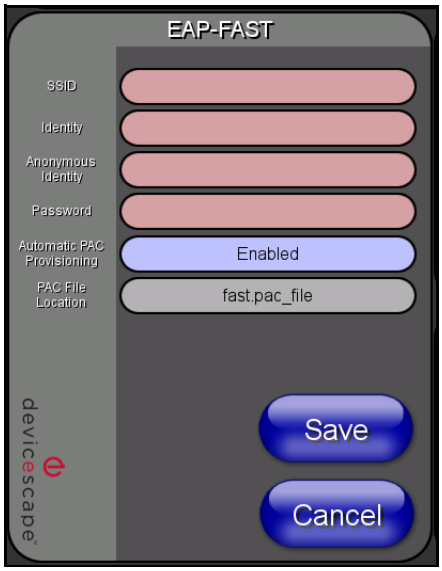


FIG. 74 Wireless Settings page - EAP-FAST Settings

EAP-FAST Settings	
SSID (Service Set Identifier):	Opens an on-screen keyboard to enter the SSID name used on the target WAP. The SSID is a unique name used by the WAP, and is assigned to all panels on that network. An SSID is required by the WAP before the panel is permitted to join the network. • The SSID is case sensitive and must not exceed 32 characters. • Make sure this setting is the same for all points in your wireless network. • NXA-WAP200Gs use **AMX** as their default SSID. • With EAP security, the SSID of the WAP *must* be entered. If it is left blank, the panel will try to connect to the first access point detected that supports EAP. However, a successful connection is not guaranteed because the detected WAP may be connected to a RADIUS server, which may not support this EAP type and/or have the proper user identities configured.
Identity:	Opens an on-screen keyboard. Enter an EAP Identity string (used by the panel to identify itself to an Authentication (RADIUS) Server). ***Note**: This information is similar to a username used to login to a secured server or workstation. This works in tandem with the Password string which is similar to the password entered to gain access to a secured workstation. Typically, this is in the form of a username such as: jdoe@amx.com.*
Anonymous Identity:	Opens an on-screen keyboard. Enter an IT provided alpha-numeric string which (similar to the username) used as the identity, but that does not represent a real user. This information is used as a fictitious name which might be seen by sniffer programs during the initial connection and setup process between the panel and the Radius server. In this way the real identity (username) is protected. Typically, this is in the form of a fictitious username such as: anonymous@amx.com
Password:	Opens an on-screen keyboard. Enter the network password string specified for the user entered within the *Identity* field (used by the panel to identify itself to an Authentication (RADIUS) Server) ***Note**: This information is similar to the password entered to gain access to a secured workstation.*

EAP-FAST Settings (Cont.)	
Automatic PAC Provisioning:	This selection toggles PAC (Protected Access Credential) Provisioning - **Enabled** *(automatic)* or **Disabled** *(manual)*. • If **Enabled** is selected, the following *PAC File Location* field is disabled, because the search for the PAC file is done automatically. • If **Disabled** is selected, the user is required to manually locate a file containing the PAC shared secret credentials for use in authentication. In this case, the IT department must create a PAC file and then transfer it into the panel using the *AMX Certificate Upload* application. Note: Even when automatic provisioning is enabled, the PAC certificate is only downloaded the first time that the panel connects to the RADIUS server. This file is then saved into the panel's file system and is then reused from then on. It is possible for the user to change a setting (such as a new Identity) that would invalidate this certificate. In that case, the panel must be forced to download a new PAC file. To do this, set Automatic PAC Provisioning to *Disabled* and then back to *Enabled*. This forces the firmware to delete the old file and request a new one.
PAC File Location:	This field is used when the previous Automatic PAC Provisioning option has been **Disabled**. • When pressed, the panel displays an on-screen PAC File Location keyboard which allows you to enter the name of the file containing the PAC shared secret credentials for use in authentication. • This field is only valid when the automatic PAC provisioning feature has been enabled via the previous field.
Save/Cancel:	• **Save** - store the new security information, apply changes, and return to the previous page. • **Cancel** - discard changes and return to the previous page.

EAP-PEAP Settings

Press the **EAP-PEAP** button to open the EAP-PEAP Settings page (FIG. 75).

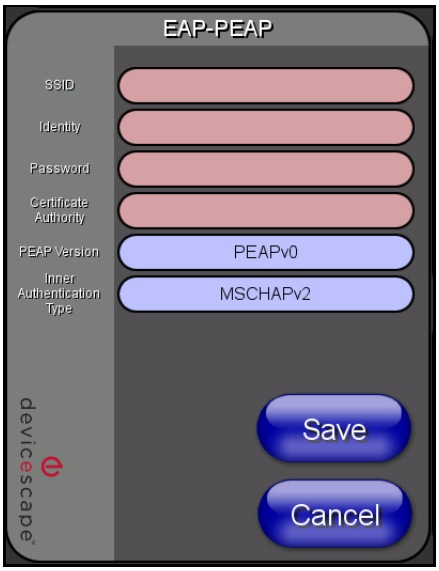


FIG. 75 Wireless Settings page - EAP-PEAP Settings

PEAP (Protected Extensible Authentication Protocol) was developed as a way to securely transmit authentication information, such as passwords, over a wireless network environment. PEAP uses only server-side public key certificates and therefore does not need a client (panel) certificate which makes the configuration and setup easier.

There are two main versions of the PEAP protocol supported by panel's DeviceScape Wireless Client:

- PEAPv0
- PEAPv1

PEAP uses inner authentication mechanisms supported by the DeviceScape Wireless Client, the most common of which are:

- MSCHAPv2 with PEAPv0
- GTC with PEAPv1

EAP-PEAP security is designed for wireless environments where it is necessary to transmit data securely over a wireless network.

EAP-PEAP Settings	
SSID (Service Set Identifier):	Opens an on-screen keyboard to enter the SSID name used on the target WAP. The SSID is a unique name used by the WAP, and is assigned to all panels on that network. An SSID is required by the WAP before the panel is permitted to join the network. • The SSID is case sensitive and must not exceed 32 characters. • Make sure this setting is the same for all points in your wireless network. • NXA-WAP200Gs use **AMX** as their default SSID. • With EAP security, the SSID of the WAP *must* be entered. If it is left blank, the panel will try to connect to the first access point detected that supports EAP. However, a successful connection is not guaranteed because the detected WAP may be connected to a RADIUS server, which may not support this EAP type and/or have the proper user identities configured.
Identity:	Opens an on-screen keyboard. Enter an EAP Identity string (used by the panel to identify itself to an Authentication (RADIUS) Server). ***Note**: This information is similar to a username used to login to a secured server or workstation. This works in tandem with the Password string which is similar to the password entered to gain access to a secured workstation. Typically, this is in the form of a username such as: jdoe@amx.com.*
Password:	Opens an on-screen keyboard. Enter the network password string specified for the user entered within the *Identity* field (used by the panel to identify itself to an Authentication (RADIUS) Server) ***Note**: This information is similar to the password entered to gain access to a secured workstation.*
Certificate Authority:	When pressed, the panel displays an on-screen Certificate Authority (CA) File Location keyboard which allows you to enter the name of the certificate authority file which is used to validate the server certificate. This field is optional. If a server certificate is used, it should first be downloaded into the panel and the *Certificate Authority* field should then be set to the name of that certificate file. No file path should be used for this setting as all certificates are stored in a specific directory that the user cannot control or change. • Use the on-screen keyboard's **Clear** button to completely erase any previously stored network path information.
PEAP Version:	When pressed, this field cycles through the choices of available PEAP: **PEAPv0, PEAPv1,** or **PEAPv1 w/peaplabel=1**.
Inner Authentication Type:	When pressed, this field cycles through the choices of available Inner Authentication mechanisms supported by the Devicescape Secure Wireless Client. The most commonly used are: **MSCHAPv2** and **GTC**. • MSCHAPv2 (*used with PEAPv0*) • TLS • GTC (*used with PEAPv1*) • OTP • MD5-Challenge

EAP-PEAP Settings (Cont.)	
Save/Cancel:	• **Save** - store the new security information, apply changes, and return to the previous page. • **Cancel** - discard changes and return to the previous page.

- Refer to the *EAP Authentication* section on page 201 for further details on these security options.
- Refer to the *Using the Site Survey tool* section on page 44 for more information on using this feature.

EAP-TTLS Settings

Press the **EAP-TTLS** button to opens the EAP-TTLS Settings page (FIG. 76).

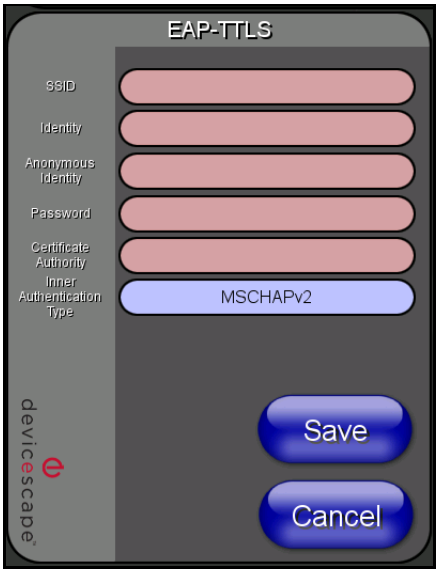


FIG. 76 Wireless Settings page - EAP-TTLS Settings

TTLS (EAP Tunneled Transport Layer Security) is an authentication method that does not use a client certificate to authenticate the panel. However. this method is more secure than PEAP because it does not broadcast the identity of the user. Setup is similar to PEAP, but differs in the following areas:

- An anonymous identity must be specified until the secure tunnel between the panel and the Radius server is setup to transfer the real identity of the user.
- There is no end-user ability to select from the different types of PEAP.
- Additional Inner Authentication choices are available to the end-user.

EAP-TTLS security is designed for wireless environments where it is necessary to have the Radius server directly validate the identity of the client (panel) before allowing it access to the network. This validation is done by tunneling a connection through the WAP and directly between the panel and the Radius server. Once the client is identified and then validated, the Radius server disconnects the tunnel and allows the panel to access the network directly via the target WAP.

EAP-TTLS Settings	
SSID (Service Set Identifier):	Opens an on-screen keyboard to enter the SSID name used on the target WAP. The SSID is a unique name used by the WAP, and is assigned to all panels on that network. An SSID is required by the WAP before the panel is permitted to join the network. • The SSID is case sensitive and must not exceed 32 characters. • Make sure this setting is the same for all points in your wireless network. • NXA-WAP200Gs use **AMX** as their default SSID. • With EAP security, the SSID of the WAP *must* be entered. If it is left blank, the panel will try to connect to the first access point detected that supports EAP. However, a successful connection is not guaranteed because the detected WAP may be connected to a RADIUS server, which may not support this EAP type and/or have the proper user identities configured.
Identity:	Opens an on-screen keyboard. Enter an EAP Identity string (used by the panel to identify itself to an Authentication (RADIUS) Server). ***Note**: This information is similar to a username used to login to a secured server or workstation. This works in tandem with the Password string which is similar to the password entered to gain access to a secured workstation. Typically, this is in the form of a username such as: jdoe@amx.com.*
Anonymous Identity:	Opens an on-screen keyboard. Enter an IT provided alpha-numeric string which (similar to the username) used as the identity, but that does not represent a real user. This information is used as a fictitious name which might be seen by sniffer programs during the initial connection and setup process between the panel and the Radius server. In this way the real identity (username) is protected. Typically, this is in the form of a fictitious username such as: anonymous@amx.com
Password:	Opens an on-screen keyboard. Enter the network password string specified for the user entered within the *Identity* field (used by the panel to identify itself to an Authentication (RADIUS) Server) ***Note**: This information is similar to the password entered to gain access to a secured workstation.*
Certificate Authority:	When pressed, the panel displays an on-screen Certificate Authority (CA) File Location keyboard which allows you to enter the name of the certificate authority file which is used to validate the server certificate. This field is optional. If a server certificate is used, it should first be downloaded into the panel and the *Certificate Authority* field should then be set to the name of that certificate file. No file path should be used for this setting as all certificates are stored in a specific directory that the user cannot control or change. • Use the on-screen keyboard's **Clear** button to completely erase any previously stored network path information.
Inner Authentication Type:	When pressed, this field cycles through the choices of available Inner Authentication mechanism supported by the Devicescape Secure Wireless Client: • MSCHAPv2 (*default because its the most common*) • MSCHAP • PAP • CHAP • EAP-MSCHAPv2 • EAP-GTC • EAP-OTP • EAP-MD5-Challenge

EAP-FAST Settings (Cont.)	
Save/Cancel:	• **Save** - store the new security information, apply changes, and return to the previous page. • **Cancel** - discard changes and return to the previous page.

- Refer to the *EAP Authentication* section on page 201 for further details on these security options.
- Refer to the *Using the Site Survey tool* section on page 44 for more information on using this feature.

EAP-TLS Settings

Press the **EAP-TLS** button to open the EAP-TLS Settings page (FIG. 77).

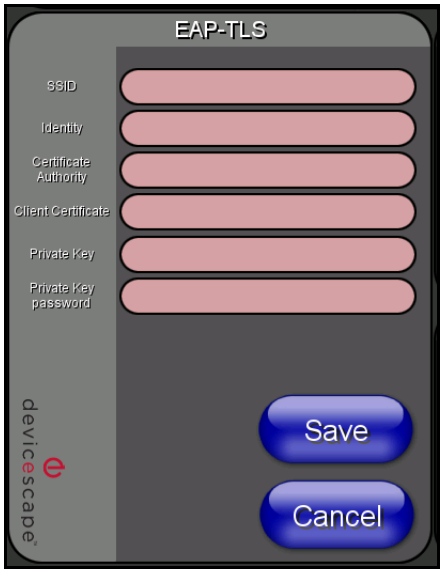


FIG. 77 Wireless Settings page - EAP-TLS Settings

TLS (Transport Layer Security) was the original standard wireless LAN EAP authentication protocol. TLS requires additional work during the deployment phase but provides additional security since even a compromised password is not enough to break into an EAP-TLS protected wireless network environment.

EAP-TLS security is designed for wireless environments where it is necessary to securely transmit data over a wireless network by adding an additional level of security protocol via the use of a private key.

EAP-TLS Settings	
SSID (Service Set Identifier):	Opens an on-screen keyboard to enter the SSID name used on the target WAP. The SSID is a unique name used by the WAP, and is assigned to all panels on that network. An SSID is required by the WAP before the panel is permitted to join the network. • The SSID is case sensitive and must not exceed 32 characters. • Make sure this setting is the same for all points in your wireless network. • NXA-WAP200Gs use **AMX** as their default SSID. • With EAP security, the SSID of the WAP *must* be entered. If it is left blank, the panel will try to connect to the first access point detected that supports EAP. However, a successful connection is not guaranteed because the detected WAP may be connected to a RADIUS server, which may not support this EAP type and/or have the proper user identities configured.

EAP-FAST Settings (Cont.)	
Identity:	Opens an on-screen keyboard. Enter an EAP Identity string (used by the panel to identify itself to an Authentication (RADIUS) Server). ***Note**: This information is similar to a username used to login to a secured server or workstation. This works in tandem with the Password string which is similar to the password entered to gain access to a secured workstation. Typically, this is in the form of a username such as: jdoe@amx.com.*
Certificate Authority:	When pressed, the panel displays an on-screen Certificate Authority (CA) File Location keyboard which allows you to enter the name of the certificate authority file which is used to validate the server certificate. This field is optional. If a server certificate is used, it should first be downloaded into the panel and the *Certificate Authority* field should then be set to the name of that certificate file. No file path should be used for this setting as all certificates are stored in a specific directory that the user cannot control or change. • Use the on-screen keyboard's **Clear** button to completely erase any previously stored network path information.
Client Certificate:	Opens an on-screen keyboard. Enter the name of the file containing the client (panel) certificate for use in certifying the identity of the client (panel). • Refer to the *Client certificate configuration* section for information regarding Client Certificates and their parameters.
Private Key:	When pressed, the panel displays an on-screen Client Private Key File Location keyboard which allows you to enter the name of the file containing the private key. • Use the on-screen keyboard's **Clear** button to completely erase any previously stored network path information.
Private Key password:	This field should only be used if the Private Key is protected with a password. If there is no password protection associated with the Private Key, then this field should be left ***blank***. • When pressed, the panel displays an on-screen Private Key Password keyboard which allows you to enter an alpha-numeric password string. • Use the on-screen keyboard's **Clear** button to completely erase any previously stored network path information.
Save/Cancel:	• **Save** - store the new security information, apply changes, and return to the previous page. • **Cancel** - discard changes and return to the previous page.

- Refer to the *EAP Authentication* section on page 201 for further details on these security options.
- Refer to the *Using the Site Survey tool* section on page 44 for more information on using this feature.

Client certificate configuration

There are several ways in which a client certificate can be configured by an IT department. The client certificate and private key can both be incorporated into one file or split into two separate files. In addition, the file format used by these files could be PEM, DER, or PKCS12. These formats are described later in this section. The following table describes how to fill in the fields for each possible case.

Client Certificate Configuration		
Certificate Configuration	**Client Certificate Field**	**Private Key Field**
Single file contains both the client certificate and the private key. *Format is:* ***PEM*** *or* ***DER****.*	Enter the file name	Enter the same file name
First file contains the client certificate, second file contains the private key. *Format is:* ***PEM*** *or* ***DER****.*	Enter the first file name	Enter the second file name
Single file contains both the client certificate and the private key. *Format is:* ***PKCS12***	Leave this field blank	Enter the file name
First file contains the client certificate, second file contains the private key. *Format is:* ***PKCS12***	not supported	not supported

AMX supports the following security certificates

- PEM (Privacy Enhanced Mail)
- DER (Distinguished Encoding Rules)
- PKCS12 (Public Key Cryptography Standard #12)

NOTE

PKCS12 files are frequently generated by Microsoft certificate applications. Otherwise, PEM is more common.

Certificate files frequently use 5 file extensions. It can be confusing because there is not a one to one correspondence. The following table shows the possible file extension used for each certificate type:

Certificates and their Extensions	
Certificate Type	**Possible File Extensions**
PEM	.cer .pem .pvk
DER	.cer .der
PKCS12	.pfx

It is important to note which certificate types are supported by the different certificate fields used on the configuration screens (PEAP, TTLS, and TLS). The following table outlines the firmware fields and their supported certificate types.

Certificate Types Supported by the Modero Firmware	
Configuration Field Name	**Certificate File Type Supported**
Certificate Authority field	PEM and DER
Client Certificate field	PEM and DER
Private Key field	.PEM, DER, and PKCS12

Calibration Page

This page (FIG. 78) allows you to calibrate the touch panel using a pre-selected touch driver.

- Press and hold the grey Front Setup Access button (below the Modero LCD) for 6 seconds to access the Calibration page.
- **Press the crosshairs to calibrate the panel and return to the last active firmware page.**

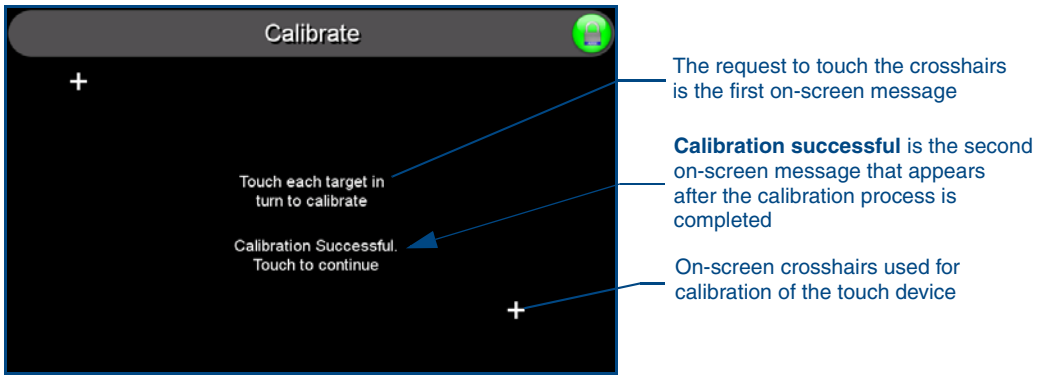


FIG. 78 Calibration page (actually 3 separate screens)

NOTE

If the calibration was improperly set and you cannot return to the Calibration page (through the panel's firmware); *you can access this firmware page via G4 WebControl where you can navigate to the Protected Setup page and press the Calibrate button through your VNC window.*
This action causes the panel to go to the Calibration page seen above, where you can physically recalibrate the actual touch panel again using the above procedures.

G4 Web Control Page

An on-board VNC (Virtual Network Computing) server allows the panel to connect to any remote PC running a VNC client. Once connected, the client can view and control the panel remotely. The options on this page allow you to enable/disable G4 Web Control functionality(FIG. 79).

FIG. 79 G4 Web Control page

Features on this page include:

G4 Web Control Page	
Back:	Saves all changes and returns to the previous page.
Connection Status icon:	The icon in the upper-right corner of each Setup page provides a constant visual indication of current connection status. ***Note**: a Lock appears on the icon if the panel is connected to a secured NetLinx Master.*
G4 Web Control Settings:	Sets the IP communication values for the touch panel:
Enable/Enabled	The Enable/Enabled button allows you to toggle between the two G4 activation settings: • **Enable** - deactivates G4 Web Control on the panel. • **Enabled** - activates G4 Web Control on the panel.
Network Interface Select	Displays **"Wireless"** when the panel is communicating via a Wireless Access Point (WAP).
Web Control Name	Use this field to enter a unique alpha-numeric string to be used as the panel's display name within the *Manage WebControl Connections* window of the NetLinx Security browser window.
Web Control Password	Use this field to enter the G4 Authentication session password required for VNC access to the panel.
Web Control Port	Enter the number of the port used by the VNC Web Server. Default = 5900.
Maximum Number of Connections	Displays the maximum number of users that can be simultaneously connected to this panel via VNC. Default = 1.
Current Connection Count	Displays the number of users currently connected to this panel via VNC.

G4 Web Control Page (Cont.)	
G4 Web Control Timeout:	Sets the length of time (in minutes) that the panel can remain idle (no cursor movements) before the G4 Web Control session is terminated. • Minimum value = 0 minutes (panel never times out) • Maximum value = 240 minutes (panel times out after 240 minutes)

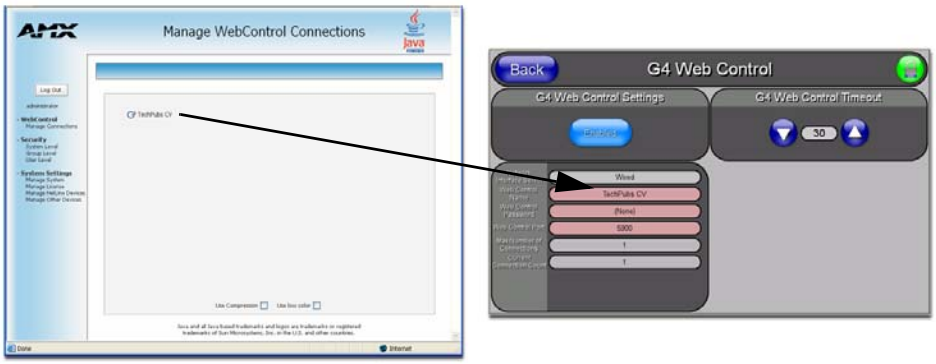


FIG. 80 Sample relationship between G4 Web Control and Mange WebControl Connections window

Refer to the *Using G4 Web Control to Interact with a G4 Panel* section on page 58 for more detailed instructions on how to use the G4 Web Control page with the new web-based NetLinx Security application.

Sensor Setup

The Sensor Setup page (FIG. 81) allows you to adjust the Light and Motion Sensor parameters on a Modero touch panel.

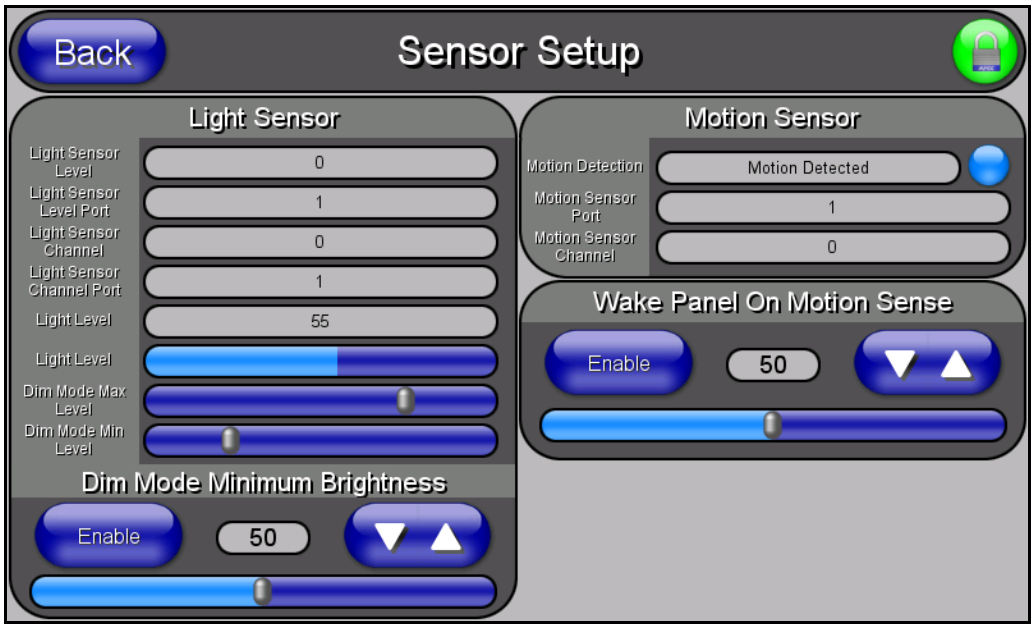


FIG. 81 Sensor Setup page

NOTE

A light level value between the Minimum and Maximum DIM Mode values delivers an average light level. The DIM mode Min Level can never exceed the DIM Mode Max Level.

The elements of the Sensor Setup page are described in the table below:

Sensor Setup Page Elements	
Back:	Saves the changes and returns you to the previously active touch panel page.
Connection Status icon:	This visual display of the connection status allows the user to have a current visual update of the panel's connection status regardless of what page is currently active. • A Lock only appears on the icon if the panel has established a connection with a currently secured target Master (*requiring a username and password*).

Sensor Setup Page Elements (Cont.)	
Light Sensor:	Allows you to monitor and alter the sensitivity of the Modero panel light sensor: • The **Light Sensor Level** field indicates the level used to report the light sensor level back to the NetLinx Master (set in TPD4) ***(read-only).*** • The **Light Sensor Level Port** field indicates the port used to report the light sensor level back to the NetLinx Master (set in TPD4) ***(read-only).*** • The **Light Sensor Channel** field indicates the level used to report the sensor channel back to the NetLinx Master (set in TPD4). It is On when you are below the Maximum dim mode level ***(read-only)***. • The **Light Sensor Channel Port** field indicates the port used to report the sensor channel back to the NetLinx Master (set in TPD4) ***(read-only).*** • The **Light Level** field provides a numeric value representing the current value of the light level detected by the on-board photo-sensor. • The Light Level bargraph displays a horizontal bargraph indicating the current value of the light level detected by the on-board photo-sensor. This bargraph provides a visual representation of the numeric value displayed within the **Light Level** field. • Use the **Dim Mode Max Level** bargraph to alter the Maximum DIM level value used to activate the DIM Mode Brightness Level (range = 0 - 100). • Use the **Dim Mode Min Level** bargraph to alter the Minimum DIM level value used to activate the DIM Mode Brightness Level (range = 0 - 100). - The position of this bargraph can never exceed that of the Dim Mode Max Level.
Dim Mode Minimum Brightness:	Allows you to alter the sensitivity of the Modero panel light sensor: • Toggle the **Enable**/**Enabled** button to either active/inactive the DIM Mode feature: - **Enable** - activates this feature. Once active (by receiving a value below the Dim Mode Min Level value), the current light level ramps to the DIM Mode value within a few seconds. - **Enabled** - (*illuminated when selected*) deactivates this feature. • Use the **DIM Mode Brightness** UP/DN buttons to alter the DIM level. - Range = 0 - 100. - The lower the value, the darker a room must be before the LCD Brightness value changes to conform to a DIM room (and vice versa with a higher value). • The **DIM Mode Minimum Brightness** bargraph indicates the current DIM Mode Brightness level. - This level corresponds to the brightness level of the LCD used when the DIM Mode is active. - The Brightness value of the panel in a DIM room (low-light) is much less than that of a Non-DIM (well to brightly-lit) where the LCD Brightness must be higher to display the screen content clearly.
Motion Sensor:	Provides the following fields: • The **Motion Detection** field displays a reactive button that changes color (illuminates) and displays the words "Motion Detected" when motion is detected by the Modero panel's front motion sensor. • The **Motion Sensor Port** field indicates the port used to report the motion sensor channel back to the NetLinx Master (set in TPD4) ***(read-only).*** • The **Motion Sensor Channel** field indicates the channel used to report the motion sensor channel back to the NetLinx Master (set in TPD4) ***(read-only).***

Sensor Setup Page Elements (Cont.)	
Wake Panel On Motion Sense:	The Wake Panel Sensitivity relates to the sensitivity of the motion sensor to detect motion and wake the panel accordingly. • Toggle the **Enable**/**Enabled** button to either active/inactive this feature: - **Enable** - activates this feature. Activating this feature reactivates the panel from a panel timeout (sleep) mode. - **Enabled** - (*illuminated when selected*) deactivates this feature and makes the panel use the specified Display Timeout value set on the Setup Page. • Use the **Wake Panel** UP/DN buttons to alter the sensitivity value. - Range = 0 - 100. • The horizontal WAKE PANEL SENSITIVITY bargraph indicates the current motion sensitivity value associated with waking the panel from a timeout.

NOTE

There is a relationship between the motion sensor and the panel sleep feature. If a panel is set to Sleep Mode, there is a time delay before the motion sensor is activated to detect motion. By creating a time delay to the detection, this allows a user to set the sleep mode and leave the panels' detection range. In this way, the panel doesn't awake immediately after the sleep is active and you move away.

Making the Most of the Automated Brightness Control Feature (DIM Mode)

Please follow the steps below to set up Automated Brightness Control:

1. Set the lighting conditions in the room to maximum (turn On all the lights).
2. Set the Maximum Panel Brightness, from the Setup page, to a comfortable level.

NOTE

Sitting in front of the panel, you should be able to comfortably see someone sitting behind the panel without being "blinded" by the panel.

3. Open the Sensors Setup page (FIG. 81) from the Protected Setup menu section.
4. Move around the panel and block the direct or indirect light from the room fixtures with your body. Take note of the drop in the lighting level being detected by the panel in response to your movements.
5. Set the Maximum brightness of the Dimmer (*Dim Mode Max Level*) below the detected drop. This will make sure that the panel does not react to variations in the lighting conditions of a normal working environment.

NOTE

The maximum (upper level) of the dimmer should be at least 15% lower than the maximum detected level.

6. Set the minimum lighting conditions in the room (not complete darkness but the minimal lighting setup, unless complete darkness is an "operational option" for the room).
7. Set the Minimum Dimmer Brightness (*Dim Mode Min Level*) to a comfortable level by sitting in front of the panel. You should be able to comfortably see someone sitting behind the panel without being "blinded" by the panel.
8. Move around the panel and block the direct or indirect light from the room fixtures with your body. Take note of the drop in the lighting level being detected by the panel in response to your movements.
9. Set the Minimum brightness of the Dimmer (*Dim Mode Max Level*) below the detected drop. This will make sure that the panel does not react to variations in the lighting conditions of a normal working environment.

NOTE

The minimum (lower level) of the dimmer should be at least 10% lower than the minimum detected level (ex: lower dimmer level at 30% if the detected lighting of the room is at 40%).

Other Settings

The Other Settings button provides a menu to select the Image Caching page, Password Setup page, or SIP Settings page. Select any option to access its page.

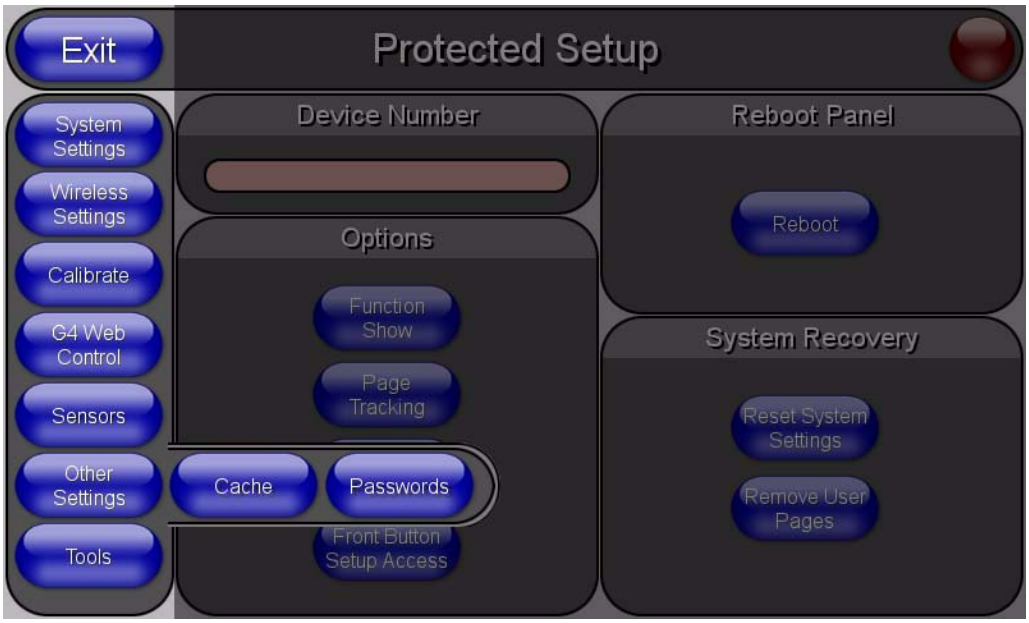


FIG. 82 Other Settings menu

Image Caching Page

The Image Caching page (FIG. 83) configures the allocation of memory for image caching. The G4 graphics engine caches images to decrease load time of previously viewed images. RAM caching is always enabled, and images (both static and dynamic) are stored in the RAM cache as they are viewed. The size of RAM cache is automatically configured to take into account available memory versus memory that may be needed by the panel later. As the RAM cache approaches its maximum size, the oldest items in the cache may be discarded to make room for newer items. If Flash caching is enabled, dynamic images that would have been discarded will actually be moved to Flash, since it is typically faster to retrieve images on Flash than across a network (although it is slower than RAM cache). Note that since static images are already stored on Flash, they are never moved to the Flash cache, so Flash caching applies only to dynamic images. Images in Flash cache are moved back to RAM cache the next time they are viewed. As the Flash cache approaches its maximum size, the least recently used items may be discarded to make room for new items.

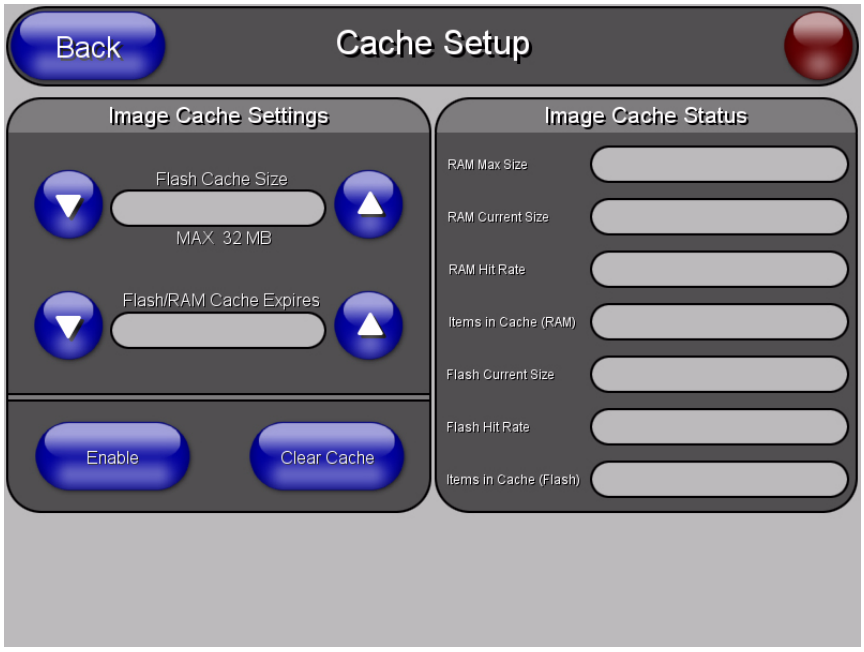


FIG. 83 Image Caching Page

The elements of this page include:

Image Caching Page Elements	
Back:	Saves all changes and returns to the previous page.
Connection Status icon:	The icon in the upper-right corner of each Setup page provides a constant visual indication of current connection status. ***Note**: a Lock appears on the icon if the panel is connected to a secured NetLinx Master.*

Image Caching Page Elements	
Image Cache Settings:	Allocates Flash memory for image caching.
Flash Cache Size	Press the Up and Down arrows to add and remove memory. Flash memory allocation cannot exceed the amount of Flash memory on the panel.
Flash/RAM Cache Expires	Press the Up and Down arrows to change the amount of time the images stay in cache memory. The options are: • Never • 2 Hours • 8 Hours • 1 Day • 2 Days • 5 Days
Enable:	Press this button to toggle the image Flash cache option On and Off.
Clear Cache:	Press this button to clear both the Flash and RAM cache of all stored images.
Image Cache Status:	The status of the memory available versus in use.
RAM Max Size	The maximum amount of memory available for all image caching.
RAM Current Size	The memory that is currently in use for caching static and dynamic images.
RAM Hit Rate	The percentage of image requests (static and dynamic) satisfied by accessing the cache. 100 * (# of cache hits) / (# of cache hits + # of cache misses) # of cache hits - the number of times an image was requested that the image was found in the cache # of cache misses - the number of times an image was requested that the image could not be found in the cache, and the image had to either be loaded from flash or obtained via the network (for dynamic images). It is considered a RAM Cache Miss even if the image is subsequently found in flash cache.
Items in Cache (RAM)	The number of images that are currently stored in the RAM cache.
Flash Current Size	The maximum flash space allocated for image caching. Flash space is used for caching only when there is not enough available memory in the RAM cache for a newly requested image (it is used only for dynamic images).
Flash Hit Rate	The percentage of image requests (dynamic only) that are satisfied by accessing the flash cache. 100 * (# of flash cache hits) / (# of flash cache hits + # of flash cache misses) # of flash cache hits - # of times a dynamic image could not be found in RAM cache but was found in flash cache # of flash cache misses - # of times a dynamic image could not be found in either RAM or flash cache. RAM cache hits are not relevant in this calculation.
Items in Cache (Flash)	The number of images that are currently stored in the Flash cache.

Setting the image cache

In the *Protected Setup* page:

1. Press the **Cache** button in the *Protected Setup Navigation Buttons* section. This opens the *Image Cache* page.
2. Set the cache expiration in the field *Flash/RAM Cache Expires*. The Up and Down arrows increment through the available time frames.
3. Press the **Enable** button to turn on image caching. The button appears illuminated when enabled.

You can allocate Flash memory for image caching, but RAM cache is always enabled.

Select the Up and Down arrows for the field *Flash Cache Size* to increase or reduce the amount of Flash memory used; the maximum amount of flash that can be allocated for caching is 75% of available flash.

Clearing the image cache

In the *Protected Setup* page:

1. Press the **Cache** button in the *Protected Setup Navigation Buttons* section. This opens the *Image Cache* page.
2. Press **Clear Cache**. This clears all image cache currently stored on the panel (both Flash and RAM).

Checking image cache status

In the *Protected Setup* page:

Press the **Cache** button in the *Protected Setup Navigation Buttons* section. This opens the *Image Cache* page. All status information is located in the *Image Cache Status* section of the page.

Password Setup Page

The Password Setup page (FIG. 84) centers around the properties used to assign passwords for the Modero panel pages.

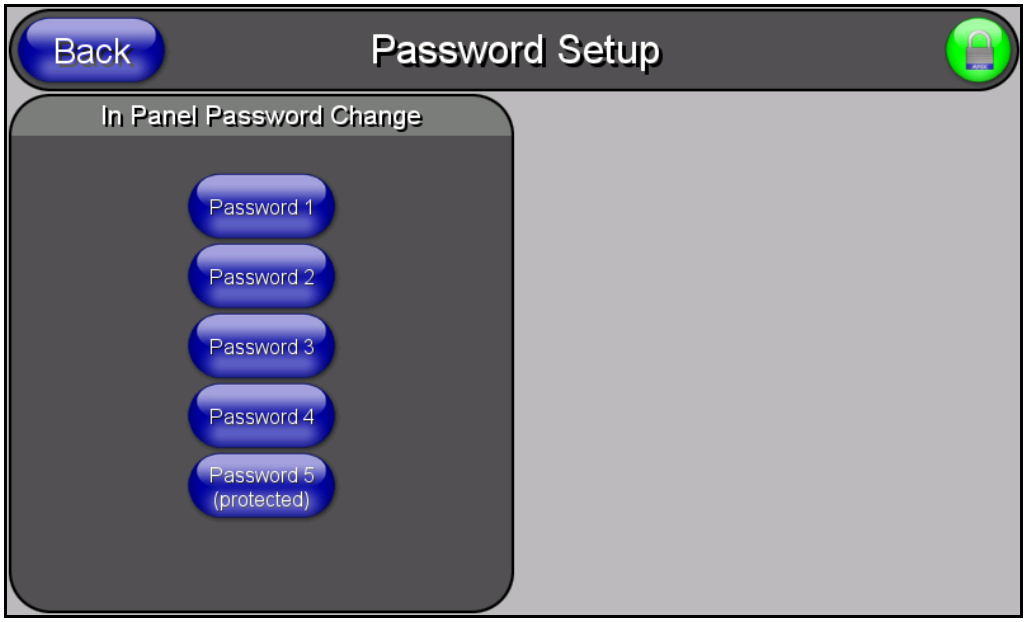


FIG. 84 Password Setup page

The elements of the Password Setup page are described in the table below:

Password Setup Page Elements	
Back:	Saves the changes and returns you to the previously active touch panel page.
Connection Status icon:	This visual display of the connection status allows the user to have a current visual update of the panel's connection status regardless of what page is currently active. • A Lock only appears on the icon if the panel has established a connection with a currently secured target Master (*requiring a username and password*).
In Panel Password Change:	Accesses the alphanumeric values associated to particular password sets. • PASSWORD 1, 2, 3, 4, 5 (protected) buttons open a keyboard where you can enter alphanumeric values associated to a selected password group. • Clearing Password #5 removes the need to enter a password before accessing the Protected Setup page.

SIP Settings Page

The options on the SIP Settings page (FIG. 85) enable you to establish network settings for using your touch panel as an IP phone. With a CSG SIP Communications Gateway (**FG2182-01, -02, -03**), you can use your touch panel to make and receive local, long distance, and international phone calls, and have access to phone features like call waiting, caller ID, call forwarding, call queuing, and voice mail. Setting up your touch panel as a telephone requires that you set it up as one in the CSG SIP Communications Gateway. Refer to the *CSG SIP Communications Gateway Operation/Reference Guide* for information on setting up your touch panel to work as a telephone.

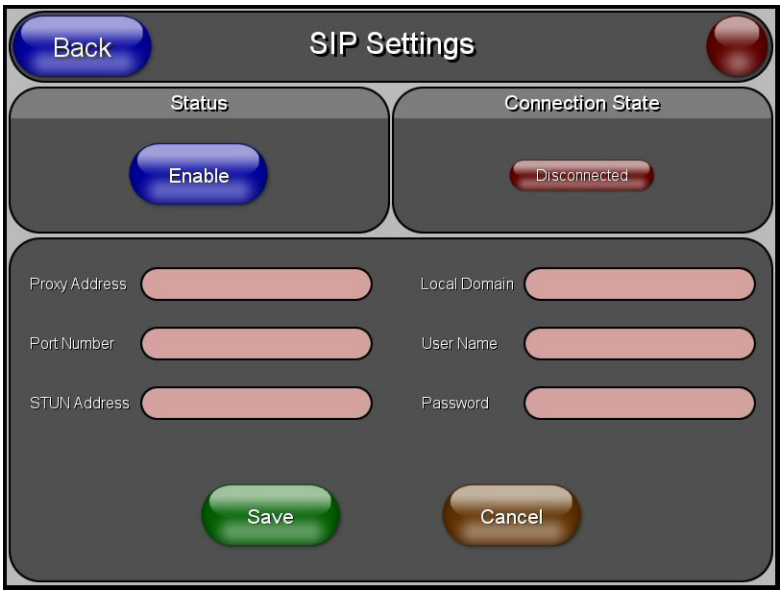


FIG. 85 SIP Settings page

You may need to load a Duet module to enable the touch panel to receive SIP calls. The Duet module translates between the standard interface and the device protocol. It parses the buffer for responses from the device, sends strings to control the device, and receives commands from the UI module or telnet sessions. Refer to the documentation supplied with the Duet Module for more details.

NOTE

A sample UI module is provided in the module package. It is not intended to cover every possible application, but can be expanded as needed by a dealer to meet the requirements of a particular installation.

Features on this page include:

SIP Settings Page	
Back:	Saves all changes and returns to the previous page.
Connection Status icon:	The icon in the upper-right corner of each Setup page shows online/offline state of the panel to the master. • Bright red - disconnected • Bright green - connected. Blinks when a blink message is received to dark green every 5 seconds for half a second then go back to bright green. • Bright yellow - panel missed a blink message from the master. It will remain yellow for 3 missed blink messages and then turn red. It will return to green when a blink message is received. ***Note**: A lock appears on the icon if the panel is connected to a secured NetLinx Master.*
Status:	This option enables the SIP Stack on startup. If you disable this option, the panel will not attempt to read the rest of the configuration and will not register with a proxy server. However, point-to-point SIP will still be enabled allowing for existing intercom functionality.
Connection State:	This option displays whether you are connected to the proxy server.
Proxy Address:	This option enables you to enter the IP address or DNS name of the proxy server that you want to use to register.
Port Number:	The option displays the port you use to connect to the proxy server. The standard SIP port is 5060, but some providers use different ports.
STUN Address:	This option enables you to enter the IP address or DNS name of the Simple Traversal of UDP through NATs (STUN) server. This field is optional.
Local Domain:	This is the realm used for authentication. This field is optional.
User Name:	This option enables you to enter the user name used for authentication to the proxy server. Normally, the user name is the same as the phone number assigned to the extension you are using. This field is optional.
Password:	This option enables you to enter the password for the user at the proxy server. This field is optional.

Tools

The Tools button provides a menu to select either the *Panel Logs Page* section on page 119, the *Panel Statistics Page* section on page 120, or the *Connection Utility Page* section on page 122. Select any of the options to access that page.

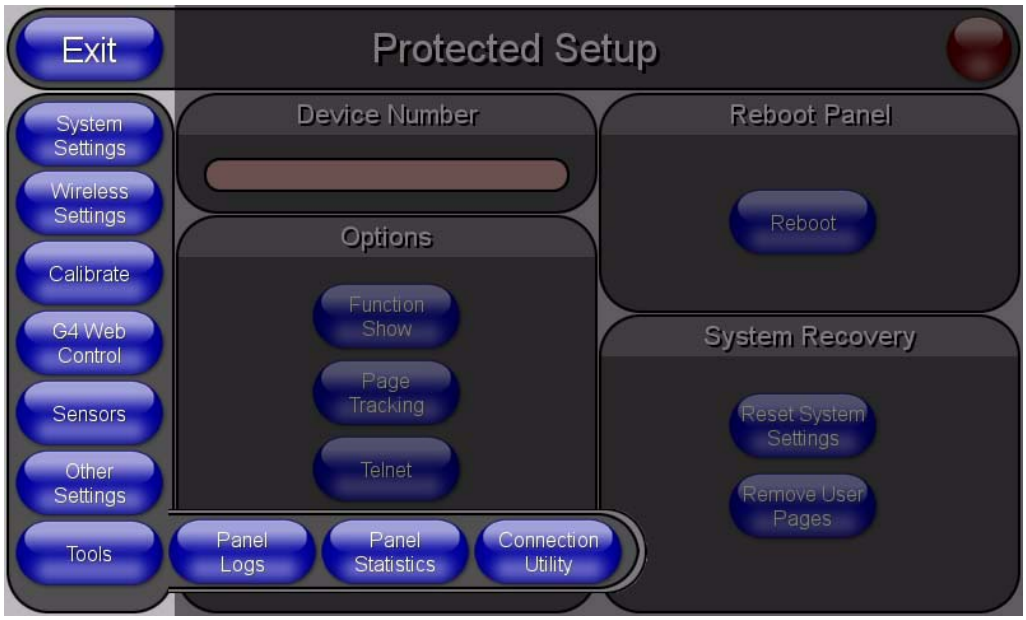


FIG. 86 Tools menu

Panel Logs Page

The options on the Panel Logs page allow you to view and track the connection history of the panel (FIG. 87).

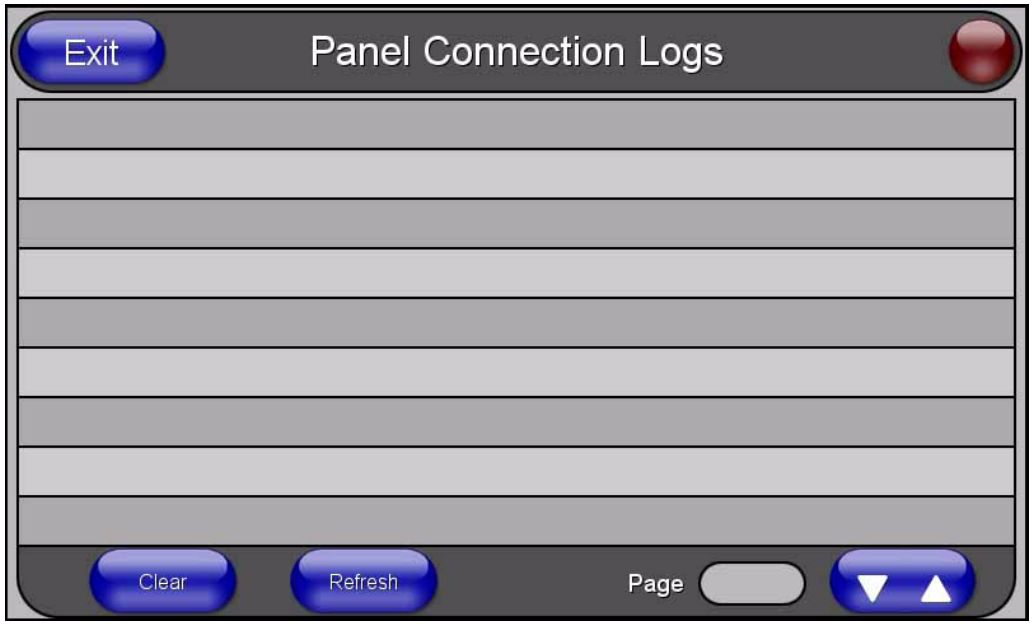


FIG. 87 Panel Logs page

Features on this page include:

Panel Logs Page	
Back:	Saves all changes and returns to the previous page.
Connection Status icon:	The icon in the upper-right corner of each Setup page shows online/offline state of the panel to the master. • Bright red - disconnected • Bright green - connected. Blinks when a blink message is received to dark green every 5 seconds for half a second then go back to bright green. • Bright yellow - panel missed a blink message from the master. It will remain yellow for 3 missed blink messages and then turn red. It will return to green when a blink message is received. ***Note**: a Lock appears on the icon if the panel is connected to a secured NetLinx Master.*
Connection Logs	A history of all connections, attempts, and failures for the panel.
Clear	Clears the Connection Logs history.
Refresh	Refreshes the Connection Logs history.
Page	Indicates the current page of the Connection Logs. Use the Up and Down arrows to move from one page to the next.

Checking the Panel Connection Logs

1. Press the **Tools** button in the *Protected Setup Navigation Buttons* section. This opens the *Tools* menu.
2. Within the *Tools* menu, press the **Panel Logs** button. All connection data is contained in the section *Connection Logs*.

Refreshing the Panel Connections Log

1. Press the **Tools** button in the *Protected Setup Navigation Buttons* section. This opens the *Tools* menu.
2. Within the *Tools* menu, press the **Panel Logs** button.
3. Push the **Refresh** button.

Clearing the Panel Connections Log

1. Press the **Tools** button in the *Protected Setup Navigation Buttons* section. This opens the *Tools* menu.
2. Within the *Tools* menu, press the **Panel Logs** button.
3. Push the **Clear** button.
4. Confirm your selection.

Panel Statistics Page

The options on the Panel Statistics page allow you to track the connection status for the panel. The *Panel Statistics* page tracks ICSP messages, Blink messages, Ethernet connection statistics, and Wireless connection statistics (FIG. 84).

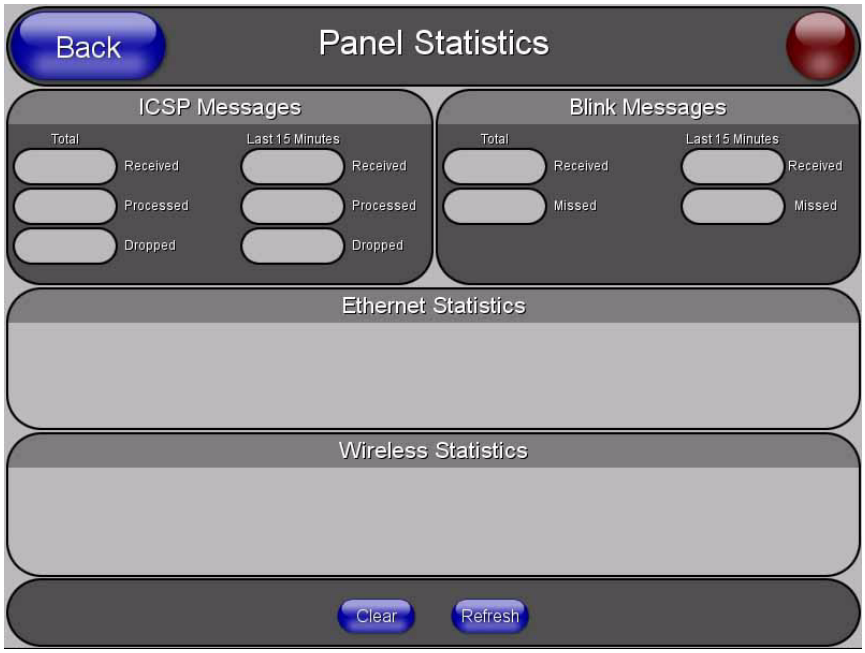


FIG. 88 Panel Statistics page

Features on this page include:

Panel Statistics Page	
Back:	Saves all changes and returns to the previous page.
Connection Status icon:	The icon in the upper-right corner of each Setup page shows online/offline state of the panel to the master. • Bright red - disconnected • Bright green - connected. Blinks when a blink message is received to dark green every 5 seconds for half a second then go back to bright green. • Bright yellow - panel missed a blink message from the master. It will remain yellow for 3 missed blink messages and then turn red. It will return to green when a blink message is received. ***Note**: a Lock appears on the icon if the panel is connected to a secured NetLinx Master.*
ICSP Messages	Messages sent between the master and the touch panel; it is the protocol they use to communicate to each other.
Total	• Received - The total ICSP messages received by the panel. • Processed - The total ICSP messages processed by the panel. • Dropped - The total ICSP messages dropped by the panel.
Last 15 Minutes	• Received - The total ICSP messages received by the panel in the last 15 minutes. • Processed - The total ICSP messages processed by the panel in the last 15 minutes. • Dropped - The total ICSP messages dropped by the panel in the last 15 minutes.
Blink Messages	The master sends this message once every 5 seconds to all connected devices.
Total	• Received - The total Blink messages received by the panel. • Missed - The total Blink messages missed by the panel.
Last 15 Minutes	• Received - The total Blink messages received by the panel in the last 15 minutes. • Missed - The total Blink messages missed by the panel in the last 15 minutes.
Ethernet Statistics	The Ethernet connection statistics for the panel.

Panel Statistics Page (Cont.)	
Wireless Statistics	The Wireless connection statistics for the panel.
Clear	Clears all panel connection statistics.
Refresh	Refreshes all panel connection statistics.

Checking the Panel Statistics

1. Press the **Tools** button in the *Protected Setup Navigation Buttons* section. This opens the *Tools* menu.
2. Within the *Tools* menu, press the **Panel Statistics** button. All connection statistics are contained on this page, e.g., *Received, Processed, and Dropped ICSP Messages*.

Refreshing the Panel Statistics

1. Press the **Tools** button in the *Protected Setup Navigation Buttons* section. This opens the *Tools* menu.
2. Within the *Tools* menu, press the **Panel Statistics** button.
3. Push the **Refresh** button.

Clearing the Panel Statistics

1. Press the **Tools** button in the *Protected Setup Navigation Buttons* section. This opens the *Tools* menu.
2. Within the *Tools* menu, press the **Panel Statistics** button.
3. Push the **Clear** button.
4. Confirm your selection.

Connection Utility Page

The options on the Connection Utility page allow you to utilize your panel as a site survey tool. While in this page, move around your wireless network coverage area and see if there are any weak points within the spaces between your WAPs (FIG. 84).

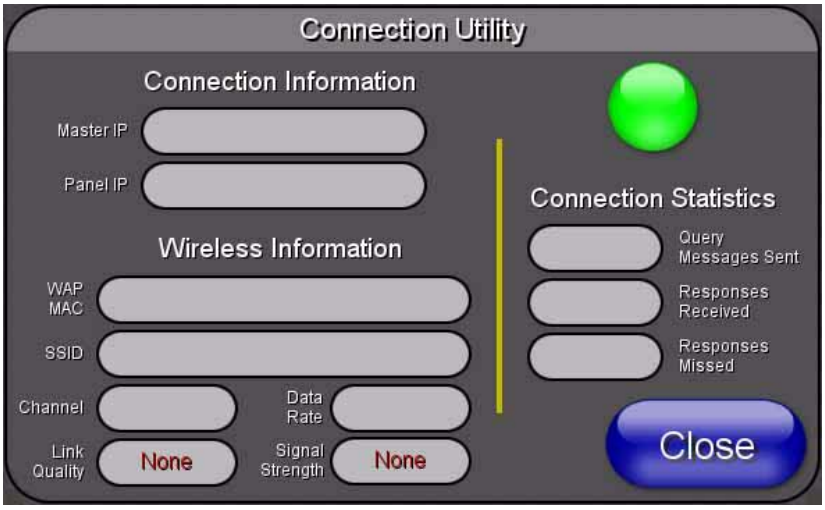


FIG. 89 Connection Utility page

Features on this page include:

Connection Utility Page	
Close:	Closes the *Connection Utility* popup.
Connection Status icon:	The icon in the upper-right corner of the utility provides a constant visual i indication of current connection status. A message is sent to the master once per second and expects a response. • If it is received the button stays green. • If it is missed the button goes yellow. • After three misses (3 seconds) it will go red until a response from the master is received, and then it will be green again. Once per second, a user can know whether they are standing in a good wireless area (all green), an area of limited coverage (lots of yellow, some green, some red), or an area with no coverage (all red).
Connection Information	
Master IP	The IP Address for the connected master.
Panel IP	The IP Address for the panel.
Wireless Information	
WAP MAC	The MAC Address for the WAP currently in use. If the MAC Address changes, it means the panel has switched/roamed to a different access point. This can be used to determine coverage for each access point and help isolate "brown" areas where coverage is minimal or non-existent, and thus require another access installed.
SSID	Displays the currently used SSID of the target WAP.
Channel	The RF channel being used for connection to the WAP (*read -only*).
Data Rate	The data rate (in Mbps) at which the panel is currently communicating with the target WAP. ***Note**: Data rates for 802.11b communication are: 1, 2, 5.5, and 11 Mbps.*
Link Quality	Displays the quality of the link from the wireless NIC to the Wireless Access Point (direct sequence spread spectrum) in real time (*None*, *Poor*, *Fair*, *Good*, *Very Good*, and *Excellent*). • Even when link quality is at its lowest you still have a connection, and the ability to transmit and receive data, even if at lower speeds. ***Note:** "Link Quality" and "Signal Strength" are applicable to RF connections only. It is possible to have an RF signal to a WAP, but be unable to communicate with it because of either incorrect IP or encryption settings.*
Signal Strength	This indicator displays a description of the signal strength from the Wireless Access Point connection in real time (*None*, *Poor*, *Fair*, *Good*, *Very Good*, and *Excellent*). SNR (Signal Noise Ratio) is a measure of the relative strength of a wireless RF connection. Given this value and the link quality above, you can determine the noise level component of the SNR. For example, if signal strength is high but the link quality is low, then the cause of the link degradation is noise. However, if signal strength is low and link quality is low the cause would simply be signal strength.
Connection Statistics	
Query Messages Sent	The number of messages sent from the panel to the master.
Responses Received	The number of responses the panel has received from the master.
Responses Missed	The number of expected responses from the master to the panel missed.

Using the Connection Utility

1. Press the **Tools** button in the *Protected Setup Navigation Buttons* section. This opens the *Tools* menu.
2. Within the *Tools* menu, press the **Connection Utility** button. This launches the *Connection Utility* pop-up window.
3. Move the panel throughout your wireless network, and changes within the utility. The *Connection Information* notes the IP of the connected master and the IP of your panel. The *Wireless Information* indicates the current wireless connection method for the panel, e.g., the MAC Address for the WAP currently in use. The *Connection Statistics* show the current quality of the panel connection.
4. Push **Close** when you are done using the site survey tool.

EAP Security & Server Certificates

Overview

The following EAP types all support a server certificate:

- EAP-PEAP
- EAP-TTLS
- EAP-TLS

All three of these certificate-using security methods are documented in the following sections. EAP Authentication goes a step beyond just encrypting data transfers, but also requires that a set of credentials be validated before the client (panel) is allowed to connect to the rest of the network (FIG. 90). Below is a description of this process. It is important to note that there is no user intervention necessary during this process. It proceeds automatically based on the configuration parameters entered into the panel.

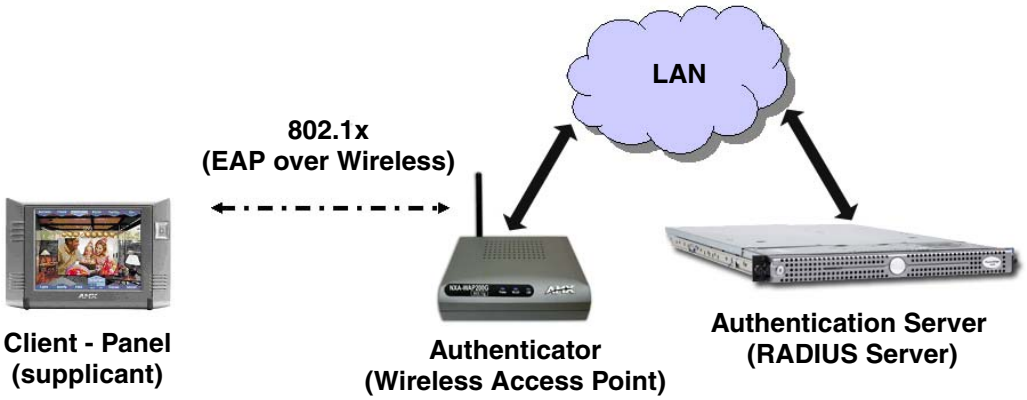


FIG. 90 EAP security method in process

A server certificate file uses a certificate that is installed in a panel so that the RADIUS server can be validated before the panel tries to connect to it. The field name associated with this file is *Certificate Authority.*

If a server certificate is used, it should first be downloaded into the panel and the *Certificate Authority* field should then be set to the name of that certificate file. No file path should be used for this setting as all certificates are stored in a specific directory that the user cannot control or change. The most secure connection method uses a server certificate.

If no server certificate will be used then, this field should be left blank. If the field contains a file name, then a valid certificate file with the same file name must be previously installed on the panel. Otherwise the authentication process will fail.

Full Duplex Intercom

Overview

VoIP technology gives users the ability to instantly create a high-quality, digital home/office intercom network with no additional equipment required. By utilizing VoIP intercom, system integration is simple and calls sound incredibly clear.

Incorporating an intercom capable panel into your NetLinx system

Download the module for the intercom panel from **www.amx.com**, and include it in your NetLinx project file. For searching purposes, the module *manufacturer* is **AMX** and the *model* is **Intercom**.

NOTE

The intercom module will only work with AMX intercom capable panels.

Panel Intercom Configuration

Setup

The setup page allows you to set the session timeout for intercom calls, toggle intercom auto-answer on and off, and provides access to the *Advanced Setup* page.

FIG. 91 Intercom Setup Page

Setting the Intercom Session Timeout

1. Select the **Setup** button on your intercom page.
2. Press the up or down arrows to increment the timeout up by 1 second in each direction. If your call exceeds your session timeout the panel provides you with a popup (FIG. 92) to extend the session.

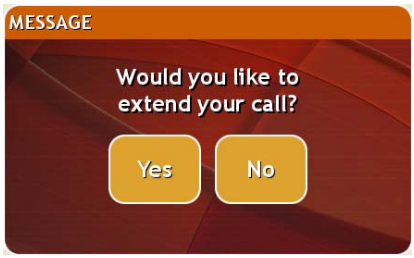


FIG. 92 Extend Call Popup

3. Press **Exit** when you are finished.

Setting Intercom Auto Answer

1. Select the **Setup** button on your intercom page.
2. Press the button beneath *Auto-Answer* to toggle the option. The button indicates its current state.
3. Press **Exit** when you are finished.

Advanced Setup

The intercom's advanced setup pages are accessed through the intercom setup pages. The advanced pages allow you to set the panel intercom to be monitored, to monitor other intercom panels, and to name the panel. It is important to name the intercom panel; the name is displayed in other panels' intercom call directory pages.

FIG. 93 Intercom Advanced Setup Page

Allowing a panel to be monitored

1. Select the **Setup** button on your intercom page.
2. On the intercom setup page, press **Advanced Setup**. This launches the password numeric keypad.
3. Enter the password and press **Done**. The default password is *Password 4* of the panel's firmware *Password Setup*.
4. Press the button beneath *Allow This Panel to be Monitored* to toggle the option. The button indicates its current state. (FIG. 94)

FIG. 94 Room Monitored

5. Press **Back** to return to the intercom setup pages.
6. Press **Exit** when you are finished.

Allowing a panel to monitor

1. Select the **Setup** button on your intercom page.
2. On the intercom setup page, press **Advanced Setup**. This launches the password numeric keypad.
3. Enter the password and press **Done**. The default password is *Password 4* of the panel's firmware *Password Setup*.
4. Press the button beneath *Allow This Panel to Monitor* to toggle the option. The button indicates its current state. If you attempt to monitor a panel that has not given permission to be monitored, your panel provides the popup in FIG. 95.

FIG. 95 Privacy Enabled

5. Press **Back** to return to the intercom setup pages.
6. Press **Exit** when you are finished.

Naming a panel

1. Select the **Setup** button on your intercom page.
2. On the intercom setup page, press **Advanced Setup**. This launches the password numeric keypad.
3. Enter the password and press **Done**. The default password is *Password 4* of the panel's firmware *Password Setup*.
4. Press in the area under *Panel Name*. This launches a on screen keyboard.
5. Type the name of the panel and press **Done**. This is the name that is displayed in other panels' intercom call directory pages.
6. Press **Back** to return to the intercom setup pages.

7. Press **Exit** when you are finished.

Sample Intercom Page

The module for duplex intercom capable panels includes user pages. While you can create your own intercom directory page (see *Creating Intercom Pages* section on page 133), it is possible to use the panel with the page below.

FIG. 96 Sample Intercom Page

Sample Intercom Page					
No.	**Name**	**Description**	**Channel Port:Code**	**Address Port:Code**	**Level Port:Code**
1	Room Name	The name of the panel as it appears in other intercom directories. See *Naming a panel* section on page 129.		0:265	
2	Page All	Pages all connected intercom panels.	1:6		
3	Place Call	Initiates an intercom call to a panel.	1:7		
4	End Call	Ends an intercom call to a panel.	1:8		
5	Privacy Off	Toggles the privacy option of the intercom. When enabled, other panels cannot contact the panel.	1:9		
6	Monitor Room	Enables the panel to monitor another room's intercom panel.	1:19		

Sample Intercom Page (Cont.)					
No.	**Name**	**Description**	**Channel Port:Code**	**Address Port:Code**	**Level Port:Code**
7	Panel Directory Room Name	The name of a panel in the intercom directory. You can call the panel, enact privacy against the panel and monitor the panel.	1:1	1:1	
8	Panel Directory Room Name	The name of a panel in the intercom directory. You can call the panel, enact privacy against the panel and monitor the panel.	1:2	1:2	
9	Panel Directory Room Name	The name of a panel in the intercom directory. You can call the panel, enact privacy against the panel and monitor the panel.	1:3	1:3	
10	Panel Directory Room Name	The name of a panel in the intercom directory. You can call the panel, enact privacy against the panel and monitor the panel.	1:4	1:4	
11	Panel Directory Room Name	The name of a panel in the intercom directory. You can call the panel, enact privacy against the panel and monitor the panel.	1:5	1:5	
12	Call Panel	Display only; indicates the panel is currently in a call.	1:21		
13	Call Panel	Display only; indicates the panel is currently in a call.	1:24		
14	Call Panel	Display only; indicates the panel is currently in a call.	1:27		
15	Call Panel	Display only; indicates the panel is currently in a call.	1:30		
16	Call Panel	Display only; indicates the panel is currently in a call.	1:33		
17	Panel Privacy	Display only; indicates the panel has privacy enabled.	1:22		
18	Panel Privacy	Display only; indicates the panel has privacy enabled.	1:25		
19	Panel Privacy	Display only; indicates the panel has privacy enabled.	1:28		
20	Panel Privacy	Display only; indicates the panel has privacy enabled.	1:31		
21	Panel Privacy	Display only; indicates the panel has privacy enabled.	1:34		
22	Monitor Panel	Display only; indicates the panel is being monitored by another panel.	1:23		
23	Monitor Panel	Display only; indicates the panel is being monitored by another panel.	1:26		

Sample Intercom Page (Cont.)					
No.	**Name**	**Description**	**Channel Port:Code**	**Address Port:Code**	**Level Port:Code**
24	Monitor Panel	Display only; indicates the panel is being monitored by another panel.	1:29		
25	Monitor Panel	Display only; indicates the panel is being monitored by another panel.	1:32		
26	Monitor Panel	Display only; indicates the panel is being monitored by another panel.	1:35		
27	Intercom Microphone Level	A Bargraph in TPDesign4 that sets the volume of the intercom microphone.			0:10
28	Intercom Sound Level	A Bargraph in TPDesign4 that sets the volume of the intercom speaker.			0:9
29	Call Status Button	Displays status of calls, e.g., incoming caller id, connected, rejected.		1:10	
30	Navigate Up	Increments the intercom directory up.	1:13		
31	Navigate Down	Increments the intercom directory down.	1:14		
32	Intercom Setup Page	Navigates the intercom panel to the intercom *Setup page*. This requires a standard page flip to *Setup*.			

Answering an incoming call

The provided intercom pages include an answering popup window. The popup page indicates the name of the panel calling and two options:

- **Answer** - Pressing this button opens the intercom session with the other panel.
- **Ignore** - Pressing this button denies the intercom session with the other panel.

FIG. 97 Answer Call

To answer a call:

In the popup window, press the **Answer** button.

Creating Intercom Pages

The easiest method of creating your own intercom pages is to start with the pages provided by AMX in the module download .ZIP file. You can change the aesthetics of the pages as long as the channel, address, level and links remain untouched.

For the more ambitious panel designers, the necessary intercom directory buttons and their information are contained in the Sample Intercom Page table on page 130.

Additionally, the *Setup* page, *Advanced Setup* page, and the popups can be edited. See below:

Setup			
Name	**Description**	**Channel Port:Code**	**Address Port:Code**
Auto-Answer OFF	Toggle the panel's auto-answer feature off and on.	1:12	
Session Timeout	A display of the current session timeout.		1:9
Increment Up	Increments the intercom session time up.	1:15	
Increment Down	Increments the intercom session time down.	1:16	
Room Name	The name of the panel as it appears in other intercom directories. See *Naming a panel* section on page 129.		0:265
Advanced Setup	Navigates the intercom panel to the intercom *Advanced Setup* page. This requires a standard page flip to *Advanced Setup*.		
Exit Setup	Navigates the intercom panel to the intercom directory page. This requires a standard page flip to the intercom directory.		

Advanced Setup			
Name	**Description**	**Channel Port:Code**	**Address Port:Code**
Allow Panel to be Monitored	Toggle the panel's ability to be monitored off and on.	1:11	
Allow Panel to Monitor	Toggle the panel's ability to monitor off and on.	1:10	
Room Name	The name of the panel as it appears in other intercom directories. See *Naming a panel* section on page 129.		0:265
Name Panel	Set the name of the panel as it appears in other intercom directories. (G4 Web Control: Server Name)	0:334	0:265
Back	Navigates the intercom panel to the intercom *Setup page*. This requires a standard page flip to *Setup*.		

More Time Popup			
Name	**Description**	**Channel Port:Code**	**Address Port:Code**
Confirm More Time	Select to extend intercom session beyond timeout.	1:20	

Answer Intercom Call Popup			
Name	**Description**	**Channel Port:Code**	**Address Port:Code**
Answer	Opens the intercom session with the other panel.	1:17	
Ignore	Denies the intercom session with the other panel.	1:18	
Room Name	The name of the panel as it appears in other intercom directories. See *Naming a panel* section on page 129.		1:7

Programming

Overview

You can program the touch panel, using the commands in this section, to perform a wide variety of operations using Send_Commands and variable text commands.

A device must first be defined in the NetLinx programming language with values for the Device: Port: System (in all programming examples - ***Panel*** is used in place of these values and represents all Modero panels).

Verify you are using the latest NetLinx Master and Modero firmware.
Verify you are using the latest version of NetLinx Studio and TPD4.

Button Assignments

- Button Channel Range: 1 - 4000 Button push and Feedback (per address port)
- Button Variable Text range: 1 - 4000 (per address port)
- Button States Range: 1 - 256 (0 = All states, for General buttons 1 = Off state and 2 = On state).
- Level Range: 1 - 600 (Default level value 0 - 255, can be set up to 1 - 65535)
- Address port Range: 1 - 100

These button assignments can only be adjusted in TPD4 and not on the panels themselves.

Page Commands

These Page Commands are used in NetLinx Programming Language and are case insensitive.

Page Commands	
@APG Add a specific popup page to a specified popup group.	Add the popup page to a group if it does not already exist. If the new popup is added to a group which has a popup displayed on the current page along with the new pop-up, the displayed popup will be hidden and the new popup will be displayed. Syntax: `"'@APG-<popup page name>;<popup group name>'"` Variable: popup page name = 1 - 50 ASCII characters. Name of the popup page. popup group name = 1 - 50 ASCII characters. Name of the popup group. Example: `SEND_COMMAND Panel,"'@APG-Popup1;Group1'"` Adds the popup page 'Popup1' to the popup group 'Group1'.
@CPG Clear all popup pages from specified popup group.	Syntax: `"'@CPG-<popup group name>'"` Variable: popup group name = 1 - 50 ASCII characters. Name of the popup group. Example: `SEND_COMMAND Panel,"'@CPG-Group1'"` Clears all popup pages from the popup group 'Group1'.

Page Commands (Cont.)	
@DPG Delete a specific popup page from specified popup group if it exists.	Syntax: `"'@DPG-<popup page name>;<popup group name>'"` Variable: popup page name = 1 - 50 ASCII characters. Name of the popup page. popup group name = 1 - 50 ASCII characters. Name of the popup group. Example: `SEND_COMMAND Panel,"'@DPG-Popup1;Group1'"` Deletes the popup page 'Popup1' from the popup group 'Group1'.
@PDR Set the popup location reset flag.	If the flag is set, the popup will return to its default location on show instead of its last drag location. Syntax: `"'@PDR-<popup page name>;<reset flag>'"` Variable: popup page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On. reset flag = 1 = Enable reset flag 0 = Disable reset flag Example: `SEND_COMMAND Panel,"'@PDR-Popup1;1'"` Popup1 will return to its default location when turned On.
@PHE Set the hide effect for the specified popup page to the named hide effect.	Syntax: `"'@PHE-<popup page name>;<hide effect name>'"` Variable: popup page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On. hide effect name = Refers to the popup effect names being used. Example: `SEND_COMMAND Panel,"'@PHE-Popup1;Slide to Left'"` Sets the Popup1 hide effect name to 'Slide to Left'.
@PHP Set the hide effect position.	Only 1 coordinate is ever needed for an effect; however, the command will specify both. This command sets the location at which the effect will end at. Syntax: `"'@PHP-<popup page name>;<x coordinate>,<y coordinate>'"` Variable: popup page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On. Example: `SEND_COMMAND Panel,"'@PHP-Popup1;75,0'"` Sets the Popup1 hide effect x-coordinate value to 75 and the y-coordinate value to 0.
@PHT Set the hide effect time for the specified popup page.	Syntax: `"'@PHT-<popup page name>;<hide effect time>'"` Variable: popup page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On. hide effect time = Given in 1/10ths of a second. Example: `SEND_COMMAND Panel,"'@PHT-Popup1;50'"` Sets the Popup1 hide effect time to 5 seconds.

Page Commands (Cont.)	
@PPA Close all popups on a specified page.	*If the page name is empty, the current page is used.* Same as the 'Clear Page' command in TPDesign4. Syntax: `"'@PPA-<page name>'"` Variable: page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On. Example: `SEND_COMMAND Panel,"'@PPA-Page1'"` Close all popups on Page1.
@PPF Deactivate a specific popup page on either a specified page or the current page.	*If the page name is empty, the current page is used (see example 2).* If the popup page is part of a group, the whole group is deactivated. This command works in the same way as the 'Hide Popup' command in TPDesign4. Syntax: `"'@PPF-<popup page name>;<page name>'"` Variable: popup page name = 1 - 50 ASCII characters. Name of the popup page. page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On. Example: `SEND_COMMAND Panel,"'@PPF-Popup1;Main'"` Example 2: `SEND_COMMAND Panel,"'@PPF-Popup1'"` Deactivates the popup page 'Popup1' on the current page.
@PPG Toggle a specific popup page on either a specified page or the current page.	*If the page name is empty, the current page is used (see example 2).* Toggling refers to the activating/deactivating (On/Off) of a popup page. This command works in the same way as the 'Toggle Popup' command in TPDesign4. Syntax: `"'@PPG-<popup page name>;<page name>'"` Variable: popup page name = 1 - 50 ASCII characters. Name of the popup page. page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On. Example: `SEND_COMMAND Panel,"'@PPG-Popup1;Main'"` Toggles the popup page 'Popup1' on the 'Main' page from one state to another (On/Off). Example 2: `SEND_COMMAND Panel,"'@PPG-Popup1'"` Toggles the popup page 'Popup1' on the current page from one state to another (On/Off).
@PPK Kill a specific popup page from all pages.	Kill refers to the deactivating (Off) of a popup window from all pages. If the pop-up page is part of a group, the whole group is deactivated. This command works in the same way as the 'Clear Group' command in TPDesign 4. Syntax: `"'@PPK-<popup page name>'"` Variable: popup page name = 1 - 50 ASCII characters. Name of the popup page. Example: `SEND_COMMAND Panel,"'@PPK-Popup1'"` Kills the popup page 'Popup1' on all pages.

Page Commands (Cont.)	
@PPM Set the modality of a specific popup page to Modal or NonModal.	A Modal popup page, when active, only allows you to use the buttons and features on that popup page. All other buttons on the panel page are inactivated. Syntax: `"'@PPM-<popup page name>;<mode>'"` Variable: popup page name = 1 - 50 ASCII characters. Name of the popup page. mode = NONMODAL converts a previously Modal popup page to a NonModal. MODAL converts a previously NonModal popup page to Modal. ***modal = 1 and non-modal = 0*** Example: `SEND_COMMAND Panel,"'@PPM-Popup1;Modal'"` Sets the popup page 'Popup1' to Modal. `SEND_COMMAND Panel,"'@PPM-Popup1;1'"` Sets the popup page 'Popup1' to Modal.
@PPN Activate a specific popup page to launch on either a specified page or the current page.	*If the page name is empty, the current page is used (see example 2).* If the popup page is already on, do not re-draw it. This command works in the same way as the 'Show Popup' command in TPDesign4. Syntax: `"'@PPN-<popup page name>;<page name>'"` Variable: popup page name = 1 - 50 ASCII characters. Name of the popup page. page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On. Example: `SEND_COMMAND Panel,"'@PPN-Popup1;Main'"` Activates 'Popup1' on the 'Main' page. Example 2: `SEND_COMMAND Panel,"'@PPN-Popup1'"` Activates the popup page 'Popup1' on the current page.
@PPT Set a specific popup page to timeout within a specified time.	If timeout is empty, popup page will clear the timeout. Syntax: `"'@PPT-<popup page name>;<timeout>'"` Variable: popup page name = 1 - 50 ASCII characters. Name of the popup page. timeout = Timeout duration in 1/10ths of a second. Example: `SEND_COMMAND Panel,"'@PPT-Popup1;30'"` Sets the popup page 'Popup1' to timeout within 3 seconds.
@PPX Close all popups on all pages.	This command works in the same way as the 'Clear All' command in TPDesign 4. Syntax: `"'@PPX'"` Example: `SEND_COMMAND Panel,"'@PPX'"` Close all popups on all pages.

Page Commands (Cont.)	
@PSE Set the show effect for the specified popup page to the named show effect.	Syntax: `"'@PSE-<popup page name>;<show effect name>'"` Variable: popup page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On. show effect name = Refers to the popup effect name being used. Example: `SEND_COMMAND Panel,"'@PSE-Popup1;Slide from Left'"` Sets the Popup1 show effect name to 'Slide from Left'.
@PSP Set the show effect position.	Only 1 coordinate is ever needed for an effect; however, the command will specify both. This command sets the location at which the effect will begin at. Syntax: `"'@PSP-<popup page name>;<x coordinate>,<y coordinate>'"` Variable: popup page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On. Example: `SEND_COMMAND Panel,"'@PSP-Popup1;100,0'"` Sets the Popup1 show effect x-coordinate value to 100 and the y-coordinate value to 0.
@PST Set the show effect time for the specified popup page.	Syntax: `"'@PST-<popup page name>;<show effect time>'"` Variable: popup page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On. show effect time = Given in 1/10ths of a second. Example: `SEND_COMMAND Panel,"'@PST-Popup1;50'"` Sets the Popup1 show effect time to 5 seconds.
PAGE Flip to a specified page.	Flips to a page with a specified page name. If the page is currently active, it will not redraw the page. Syntax: `"'PAGE-<page name>'"` Variable: page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On. Example: `SEND_COMMAND Panel,"'PAGE-Page1'"` Flips to page1.

Page Commands (Cont.)	
PPOF Deactivate a specific popup page on either a specified page or the current page.	*If the page name is empty, the current page is used (see example 2).* If the popup page is part of a group, the whole group is deactivated. This command works in the same way as the 'Hide Popup' command in TPDesign4. Syntax: `"'PPOF-<popup page name>;<page name>'"` Variable: popup page name = 1 - 50 ASCII characters. Name of the popup page. page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On. Example: `SEND_COMMAND Panel,"'PPOF-Popup1;Main'"` Deactivates the popup page 'Popup1' on the Main page. Example 2: `SEND_COMMAND Panel,"'PPOF-Popup1'"` Deactivates the popup page 'Popup1' on the current page.
PPOG Toggle a specific popup page on either a specified page or the current page.	*If the page name is empty, the current page is used (see example 2).* Toggling refers to the activating/deactivating (On/Off) of a popup page. This command works in the same way as the 'Toggle Popup' command in TPDesign4. Syntax: `"'PPOG-<popup page name>;<page name>'"` Variable: popup page name = 1 - 50 ASCII characters. Name of the popup page. page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On. Example: `SEND_COMMAND Panel,"'PPOG-Popup1;Main'"` Toggles the popup page 'Popup1' on the Main page from one state to another (On/Off). Example 2: `SEND_COMMAND Panel,"'PPOG-Popup1'"` Toggles the popup page 'Popup1' on the current page from one state to another (On/Off).
PPON Activate a specific popup page to launch on either a specified page or the current page.	*If the page name is empty, the current page is used (see example 2).* If the popup page is already On, do not re-draw it. This command works in the same way as the 'Show Popup' command in TPDesign4. Syntax: `"'PPON-<popup page name>;<page name>'"` Variable: popup page name = 1 - 50 ASCII characters. Name of the popup page. page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On. Example: `SEND_COMMAND Panel,"'PPON-Popup1; Main'"` Activates the popup page 'Popup1' on the Main page. Example 2: `SEND_COMMAND Panel,"'PPON-Popup1'"` Activates the popup page 'Popup1' on the current page.

Programming Numbers

The following information provides the programming numbers for colors, fonts, and borders.

Colors can be used to set the colors on buttons, sliders, and pages. The lowest color number represents the lightest color-specific display; the highest number represents the darkest display. For example, 0 represents light red, and 5 is dark red.

RGB Triplets And Names For Basic 88 Colors

RGB Values for all 88 Basic Colors				
Index No.	**Name**	**Red**	**Green**	**Blue**
00	Very Light Red	255	0	0
01	Light Red	223	0	0
02	Red	191	0	0
03	Medium Red	159	0	0
04	Dark Red	127	0	0
05	Very Dark Red	95	0	0
06	Very Light Orange	255	128	0
07	Light Orange	223	112	0
08	Orange	191	96	0
09	Medium Orange	159	80	0
10	Dark Orange	127	64	0
11	Very Dark Orange	95	48	0
12	Very Light Yellow	255	255	0
13	Light Yellow	223	223	0
14	Yellow	191	191	0
15	Medium Yellow	159	159	0
16	Dark Yellow	127	127	0
17	Very Dark Yellow	95	95	0
18	Very Light Lime	128	255	0
19	Light Lime	112	223	0
20	Lime	96	191	0
21	Medium Lime	80	159	0
22	Dark Lime	64	127	0
23	Very Dark Lime	48	95	0
24	Very Light Green	0	255	0
25	Light Green	0	223	0
26	Green	0	191	0
27	Medium Green	0	159	0
28	Dark Green	0	127	0
29	Very Dark Green	0	95	0
30	Very Light Mint	0	255	128
31	Light Mint	0	223	112
32	Mint	0	191	96
33	Medium Mint	0	159	80
34	Dark Mint	0	127	64
35	Very Dark Mint	0	95	
36	Very Light Cyan	0	255	255
37	Light Cyan	0	223	223
38	Cyan	0	191	191
39	Medium Cyan	0	159	159
40	Dark Cyan	0	127	127
41	Very Dark Cyan	0	95	95
42	Very Light Aqua	0	128	255
43	Light Aqua	0	112	223
44	Aqua	0	96	191
45	Medium Aqua	0	80	159
46	Dark Aqua	0	64	127
47	Very Dark Aqua	0	48	95

RGB Values for all 88 Basic Colors (Cont.)				
Index No.	**Name**	**Red**	**Green**	**Blue**
48	Very Light Blue	0	0	255
49	Light Blue	0	0	223
50	Blue	0	0	191
51	Medium Blue	0	0	159
52	Dark Blue	0	0	127
53	Very Dark Blue	0	0	95
54	Very Light Purple	128	0	255
55	Light Purple	112	0	223
56	Purple	96	0	191
57	Medium Purple	80	0	159
58	Dark Purple	64	0	127
59	Very Dark Purple	48	0	95
60	Very Light Magenta	255	0	255
61	Light Magenta	223	0	223
62	Magenta	191	0	191
63	Medium Magenta	159	0	159
64	Dark Magenta	127	0	127
65	Very Dark Magenta	95	0	95
66	Very Light Pink	255	0	128
67	Light Pink	223	0	112
68	Pink	191	0	96
69	Medium Pink	159	0	80
70	Dark Pink	127	0	64
71	Very Dark Pink	95	0	48
72	White	255	255	255
73	Grey1	238	238	238
74	Grey3	204	204	204
75	Grey5	170	170	170
76	Grey7	136	136	136
77	Grey9	102	102	102
78	Grey4	187	187	187
79	Grey6	153	153	153
80	Grey8	119	119	119
81	Grey10	85	85	85
82	Grey12	51	51	51
83	Grey13	34	34	34
84	Grey2	221	221	221
85	Grey11	68	68	68
86	Grey14	17	17	17
87	Black	0	0	0
255	TRANSPARENT	99	53	99

Font Styles and ID Numbers

Font styles can be used to program the text fonts on buttons, sliders, and pages. The following chart shows the default font type and their respective ID numbers generated by TPDesign4.

Default Font Styles and ID Numbers

Font ID #	Font type	Size	Font ID #	Font type	Size
1	Courier New	9	19	Arial	9
2	Courier New	12	20	Arial	10
3	Courier New	18	21	Arial	12
4	Courier New	26	22	Arial	14
5	Courier New	32	23	Arial	16
6	Courier New	18	24	Arial	18
7	Courier New	26	25	Arial	20
8	Courier New	34	26	Arial	24
9	AMX Bold	14	27	Arial	36
10	AMX Bold	20	28	Arial Bold	10
11	AMX Bold	36	29	Arial Bold	8
			32 - Variable Fonts start at 32.		

You must import fonts into a TPDesign4 project file. The font ID numbers are assigned by TPDesign4. These values are also listed in the ***Generate Programmer's Report****.*

Border Styles and Programming Numbers

Border styles can be used to program borders on buttons, sliders, and popup pages.

Border Styles and Programming Numbers

No.	Border styles	No.	Border styles
0-1	No border	10-11	Picture frame
2	Single line	12	Double line
3	Double line	20	Bevel-S
4	Quad line	21	Bevel-M
5-6	Circle 15	22-23	Circle 15
7	Single line	24-27	Neon inactive-S
8	Double line	40-41	Diamond 55
9	Quad line		

The TPDesign4 Touch Panel Design program has pre-set border styles that are user selectable.

You cannot use the following number values for programming purposes when changing border styles. TPD4 border styles can ONLY be changed by using the name.

TPD4 Border Styles by Name

No.	Border styles	No.	Border styles
1	None	22	Circle 155
2	AMX Elite -L	23	Circle 165
3	AMX Elite -M	24	Circle 175
4	AMX Elite -S	25	Circle 185
5	Bevel -L	26	Circle 195
6	Bevel -M	27	Cursor Bottom
7	Bevel -S	28	Cursor Bottom with Hole

TPD4 Border Styles by Name			
No.	**Border styles**	**No.**	**Border styles**
8	Circle 15	29	Cursor Top
9	Circle 25	30	Cursor Top with Hole
10	Circle 35	31	Cursor Left
11	Circle 45	32	Cursor Left with Hole
12	Circle 55	33	Cursor Right
13	Circle 65	34	Cursor Right with Hole
14	Circle 75	35	Custom Frame
15	Circle 85	36	Diamond 15
16	Circle 95	37	Diamond 25
17	Circle 105	38	Diamond 35
18	Circle 115	39	Diamond 45
19	Circle 125	40	Diamond 55
20	Circle 135	41	Diamond 65
21	Circle 145	42	Diamond 75
43	Diamond 85	85	Menu Bottom Rounded 65
44	Diamond 95	86	Menu Bottom Rounded 75
45	Diamond 105	87	Menu Bottom Rounded 85
46	Diamond 115	88	Menu Bottom Rounded 95
47	Diamond 125	89	Menu Bottom Rounded 105
48	Diamond 135	90	Menu Bottom Rounded 115
49	Diamond 145	91	Menu Bottom Rounded 125
50	Diamond 155	92	Menu Bottom Rounded 135
51	Diamond 165	93	Menu Bottom Rounded 145
52	Diamond 175	94	Menu Bottom Rounded 155
53	Diamond 185	95	Menu Bottom Rounded 165
54	Diamond 195	96	Menu Bottom Rounded 175
55	Double Bevel -L	97	Menu Bottom Rounded 185
56	Double Bevel -M	98	Menu Bottom Rounded 195
57	Double Bevel -S	99	Menu Top Rounded 15
58	Double Line	100	Menu Top Rounded 25
59	Fuzzy	101	Menu Top Rounded 35
60	Glow-L	102	Menu Top Rounded 45
61	Glow-S	103	Menu Top Rounded 55
62	Help Down	104	Menu Top Rounded 65
63	Neon Active -L	105	Menu Top Rounded 75
64	Neon Active -S	106	Menu Top Rounded 85
65	Neon Inactive -L	107	Menu Top Rounded 95
66	Neon Inactive -S	108	Menu Top Rounded 105
67	Oval H 60x30	109	Menu Top Rounded 115
68	Oval H 100x50	110	Menu Top Rounded 125
69	Oval H 150x75	111	Menu Top Rounded 135
70	Oval H 200x100	112	Menu Top Rounded 145
71	Oval V 30x60	113	Menu Top Rounded 155
72	Oval V 50x100	114	Menu Top Rounded 165
73	Oval V 75x150	115	Menu Top Rounded 175
74	Oval V 100x200	116	Menu Top Rounded 185
75	Picture Frame	117	Menu Top Rounded 195

TPD4 Border Styles by Name			
No.	**Border styles**	**No.**	**Border styles**
76	Quad Line	118	Menu Right Rounded 15
77	Single Line	119	Menu Right Rounded 25
78	Windows Style Popup	120	Menu Right Rounded 35
79	Windows Style Popup (Status Bar)	121	Menu Right Rounded 45
80	Menu Bottom Rounded 15	122	Menu Right Rounded 55
81	Menu Bottom Rounded 25	123	Menu Right Rounded 65
82	Menu Bottom Rounded 35	124	Menu Right Rounded 75
83	Menu Bottom Rounded 45	125	Menu Right Rounded 85
84	Menu Bottom Rounded 55	126	Menu Right Rounded 95
127	Menu Right Rounded 105	145	Menu Left Rounded 95
128	Menu Right Rounded 115	146	Menu Left Rounded 105
129	Menu Right Rounded 125	147	Menu Left Rounded 115
130	Menu Right Rounded 135	148	Menu Left Rounded 125
131	Menu Right Rounded 145	149	Menu Left Rounded 135
132	Menu Right Rounded 155	150	Menu Left Rounded 145
133	Menu Right Rounded 165	151	Menu Left Rounded 155
134	Menu Right Rounded 175	152	Menu Left Rounded 165
135	Menu Right Rounded 185	153	Menu Left Rounded 175
136	Menu Right Rounded 195	154	Menu Left Rounded 185
137	Menu Left Rounded 15	155	Menu Left Rounded 195
138	Menu Left Rounded 25		
139	Menu Left Rounded 35		
140	Menu Left Rounded 45		
141	Menu Left Rounded 55		
142	Menu Left Rounded 65		
143	Menu Left Rounded 75		
144	Menu Left Rounded 85		

"^" Button Commands

These Button Commands are used in NetLinx Studio and are case insensitive.

All commands that begin with "^" have the capability of assigning a variable text address range and button state range. **A device must first be defined in the NetLinx programming language with values for the Device: Port : System** (in all programming examples - ***Panel*** is used in place of these values).

- **Variable text ranges** allow you to target 1 or more variable text channels in a single command.
- **Button State ranges** allow you to target 1 or more states of a variable text button with a single command.
- **"."** Character is used for the 'through' notation, also the "**&**" character is used for the 'And' notation.

"^" Button Commands	
^ANI Run a button animation (in 1/10 second).	Syntax: `"'^ANI-<vt addr range>,<start state>,<end state>,<time>'"` Variable: variable text address range = 1 - 4000. start state = Beginning of button state (0= current state). end state = End of button state. time = In 1/10 second intervals. Example: `SEND_COMMAND Panel,"'^ANI-500,1,25,100'"` Runs a button animation at text range 500 from state 1 to state 25 for 10 second.
^APF Add page flip action to a button if it does not already exist.	Syntax: `"'^APF-<vt addr range>,<page flip action>,<page name>'"` Variable: variable text address range = 1 - 4000. page flip action = **Stan**[dardPage] - Flip to standard page **Prev**[iousPage] - Flip to previous page **Show**[Popup] - Show Popup page **Hide**[Popup] - Hide Popup page **Togg**[lePopup] - Toggle popup state **ClearG**[roup] - Clear popup page group from all pages **ClearP**[age] - Clear all popup pages from a page with the specified page name **ClearA**[ll] - Clear all popup pages from all pages page name = 1 - 50 ASCII characters. Example: `SEND COMMAND Panel,"'^APF-400,Stan,Main Page'"` Assigns a button to a standard page flip with page name 'Main Page'.
^BAT Append non-unicode text.	Syntax: `"'^BAT-<vt addr range>,<button states range>,<new text>'"` Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). new text = 1 - 50 ASCII characters. Example: `SEND_COMMAND Panel,"'^BAT-520,1,Enter City'"` Appends the text 'Enter City' to the button's OFF state.

"^" Button Commands (Cont.)	
^BAU Append unicode text.	Same format as ^UNI. Syntax: `"'^BAU-<vt addr range>,<button states range>,<unicode text>'"` Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). unicode text = 1 - 50 ASCII characters. Unicode characters must be entered in Hex format. Example: `SEND_COMMAND Panel,"'^BAU-520,1,00770062'"` Appends Unicode text '00770062' to the button's OFF state.
^BCB Set the border color to the specified color.	**Only if** the specified border color is not the same as the current color. ***Note**: Color can be assigned by color name (without spaces), number or R,G,B value (RRGGBB or RRGGBBAA).* Syntax: `"'^BCB-<vt addr range>,<button states range>,<color value>'"` Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). color value = Refer to theRGB Values for all 88 Basic Colors table on page 141 for more information. Example: `SEND_COMMAND Panel,"'^BCB-500.504&510,1,12'"` Sets the Off state border color to 12 (Yellow). Colors can be set by Color Numbers, Color name, R,G,B,alpha colors (RRGGBBAA) and R, G & B colors values (RRGGBB). Refer to theRGB Values for all 88 Basic Colors table on page 141.
^BCF Set the fill color to the specified color.	**Only if** the specified fill color is not the same as the current color. ***Note**: Color can be assigned by color name (without spaces), number or R,G,B value (RRGGBB or RRGGBBAA).* Syntax: `"'^BCF-<vt addr range>,<button states range>,<color value>'"` Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). color value = Refer to theRGB Values for all 88 Basic Colors table on page 141 for more information. Example: `SEND_COMMAND Panel,"'^BCF-500.504&510.515,1,12'"` `SEND_COMMAND Panel,"'^BCF-500.504&510.515,1,Yellow'"` `SEND_COMMAND Panel,"'^BCF-500.504&510.515,1,#F4EC0A63''"` `SEND_COMMAND Panel,"'^BCF-500.504&510.515,1,#F4EC0A'"` Sets the Off state fill color by color number. Colors can be set by Color Numbers, Color name, R,G,B,alpha colors (RRGGBBAA) and R, G & B colors values (RRGGBB).

"^" Button Commands (Cont.)	
^BCT Set the text color to the specified color.	**Only if** the specified text color is not the same as the current color. ***Note**: Color can be assigned by color name (without spaces), number or R,G,B value (RRGGBB or RRGGBBAA).* Syntax: `"'^BCT-<vt addr range>,<button states range>,<color value>'"` Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). color value = Refer to theRGB Values for all 88 Basic Colors table on page 141 for more information. Example: `SEND_COMMAND Panel,"'^BCT-500.504&510,1,12'"` Sets the Off state border color to 12 (Yellow). Colors can be set by Color Numbers, Color name, R,G,B,alpha colors (RRGGBBAA) and R, G & B colors values (RRGGBB).
^BDO Set the button draw order.	Determines what order each layer of the button is drawn. Syntax: `"'^BDO-<vt addr range>,<button states range>,<1-5><1-5><1-5><1-5><1-5>'"` Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). layer assignments = Fill Layer = 1 Image Layer = 2 Icon Layer = 3 Text Layer = 4 Border Layer = 5 ***Note**: The layer assignments are from bottom to top. The default draw order is* **12345**. Example: `SEND_COMMAND Panel,"'^BDO-530,1&2,51432'"` Sets the button's variable text 530 ON/OFF state draw order (from bottom to top) to Border, Fill, Text, Icon, and Image. Example 2: `SEND_COMMAND Panel,"'^BDO-1,0,12345'"` Sets all states of a button back to its default drawing order.
^BFB Set the feedback type of the button.	**ONLY works** on General-type buttons. Syntax: `"'^BFB-<vt addr range>,<feedback type>'"` Variable: variable text address range = 1 - 4000. feedback type = (None, Channel, Invert, On (Always on), Momentary, and Blink). Example: `SEND_COMMAND Panel,"'^BFB-500,Momentary'"` Sets the Feedback type of the button to 'Momentary'.

"^" Button Commands (Cont.)	
^BIM Set the input mask for the specified address.	Syntax: `"'^BIM-<vt addr range>,<input mask>'"` Variable: variable text address range = 1 - 4000. input mask = Refer to the*Text Area Input Masking* section on page 192 for character types. Example: `SEND_COMMAND Panel,"'^BIM-500,AAAAAAAAAA'"` Sets the input mask to ten 'A' characters, that are required, to either a letter or digit **(entry is required).**
^BLN Set the number of lines removed equally from the top and bottom of a composite video signal.	The maximum number of lines to remove is 240. A value of 0 will display the incoming video signal unaffected. This command is used to scale non 4x3 video images into non 4x3 video buttons. Syntax: `"'^BLN-<vt addr range>,<button states range>,<number of lines>'"` Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). number of lines = 0 - 240. Example: `SEND_COMMAND Panel,"'^BLN-500,55'"` Equally removes 55 lines from the top and 55 lines from the bottom of the video button.
^BMC Button copy command. Copy attributes of the source button to all the destination buttons.	Note that the source is a single button state. Each state must be copied as a separate command. The <codes> section represents what attributes will be copied. All codes are 2 char pairs that can be separated by comma, space, percent or just ran together. Syntax: `"'^BMC-<vt addr range>,<button states range>,<source port>,<source address>,<source state>,<codes>'"` Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). • source port = 1 - 100. • source address = 1 - 4000. • source state = 1 - 256. codes: BM - Picture/Bitmap BR - Border CB - Border Color CF - Fill Color CT - Text Color EC - Text effect color EF - Text effect FT - Font IC - Icon JB - Bitmap alignment JI - Icon alignment JT - Text alignment LN - Lines of video removed OP - Opacity SO - Button Sound TX - Text VI - Video slot ID WW - Word wrap on/off

<table>
<tr><th colspan="2">"^" Button Commands (Cont.)</th></tr>
<tr><td>^BMC (Cont.)</td><td>Example:
SEND_COMMAND Panel,"'^BMC-425,1,1,500,1,BR'"
or
SEND_COMMAND Panel,"'^BMC-425,1,1,500,1,%BR'"
Copies the OFF state border of button with a variable text address of 500 onto the OFF state border of button with a variable text address of 425.
Example 2:
SEND_COMMAND Panel,"'^BMC-150,1,1,315,1,%BR%FT%TX%BM%IC%CF%CT'"
Copies the OFF state border, font, Text, bitmap, icon, fill color and text color of the button with a variable text address of 315 onto the OFF state border, font, Text, bitmap, icon, fill color and text color of the button with a variable text address of 150.</td></tr>
<tr><td>^BMF
Set any/all button parameters by sending embedded codes and data.</td><td>Syntax:
"'^BMF-<vt addr range>,<button states range>,<data>'"
Variables:
variable text address char array = 1 - 4000.
button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
level range = 1 - 600 (level value is 1 - 65535).
data:
'%B<border style>' = Set the border style name. See theBorder Styles and Programming Numbers table on page 143.
'%B',<border 0-27,40,41> = Set the borer style number. See theBorder Styles and Programming Numbers table on page 143.
'%DO<1-5><1-5><1-5><1-5><1-5> = Set the draw order. Listed from bottom to top. Refer to the ^BDO command on page 148 for more information.
'%F',<font 1-8,10,11,20-29,32-xx> = Set the font. See theDefault Font Styles and ID Numbers table on page 143.
'%F<font 01-08,10,11,20-29,32-xx>' = Set the font. See theDefault Font Styles and ID Numbers table on page 143.
'%MI<mask image>' = Set the mask image. Refer to the ^BMI command on page 152 for more information.
'%T<text >' = Set the text using ASCII characters (empty is clear).
'%P<bitmap>' = Set the picture/bitmap filename (empty is clear).
'%I',<icon 01-9900, 0-clear>' = Set the icon using values of 01 - 9900 (icon numbers are assigned in the TPDesign4 Resource Manager tab - Slots section).
'%I<icon 01-9900, 0-clear>' = Set the icon using values of 01 - 9900 (icon numbers are assigned in the TPDesign4 Resource Manager tab - Slots section).
'%J',<alignment of text 1-9> = As shown the following telephone keypad alignment chart:
0
<table><tr><td>1</td><td>2</td><td>3</td></tr><tr><td>4</td><td>5</td><td>6</td></tr><tr><td>7</td><td>8</td><td>9</td></tr></table>Zero can be used for an absolute position
'%JT<alignment of text 0-9>' = As shown the above telephone keypad alignment chart, BUT the 0 (zero) is absolute and followed by ',<left>,<top>'
'%JB<alignment of bitmap/picture 0-9>' = As shown the above telephone keypad alignment chart BUT the 0 (zero) is absolute and followed by ',<left>,<top>'
'%JI<alignment of icon 0-9>' = As shown the above telephone keypad alignment chart, BUT the 0 (zero) is absolute and followed by ',<left>,<top>'</td></tr>
</table>

"^" Button Commands (Cont.)	
^BMF (Cont.)	*For some of these commands and values, refer to* theRGB Values for all 88 Basic Colors table on page 141. '%CF<on fill color>' = Set Fill Color. '%CB<on border color>' = Set Border Color. '%CT<on text color>' = Set Text Color. '%SW<1 or 0>' = Show/hide a button. '%ST<style>' = Button style. '%SO<sound>' = Set the button sound. '%EN<1 or 0>' = Enable/disable a button. '%WW<1 or 0>' = Word wrap ON/OFF. '%GH<bargraph hi>' = Set the bargraph upper limit. '%GL<bargraph low>' = Set the bargraph lower limit. '%GN<bargraph slider name>' = Set the bargraph slider name/Joystick cursor name. '%GC<bargraph slider color>' = Set the bargraph slider color/Joystick cursor color. '%GI<bargraph invert>' = Set the bargraph invert/noninvert or joystick coordinate (0,1,2,3). *^GIV* section on page 158 more information. '%GU<bargraph ramp up>' = Set the bargraph ramp up time in intervals of 1/10 second. '%GD<bargraph ramp down>' = Set the bargraph ramp down time in 1/10 second. '%GG<bargraph drag increment> = Set the bargraph drag increment. Refer to the ^GDI command on page 158 for more information. '%VI<video ON/OFF>' = Set the Video either ON (value=1) or OFF (value=0). '%OT<feedback type>' = Set the Feedback (Output) Type to one of the following: None, Channel,Invert, ON (Always ON), Momentary, or Blink. '%SM' = Submit a text for text area button. '%SF<1 or 0>' = Set the focus for text area button. '%OP<0-255>' = Set the button opacity to either Invisible (value=0) or Opaque (value=255). '%OP#<00-FF>' = Set the button opacity to either Invisible (value=00) or Opaque (value=FF). '%UN<Unicode text>' = Set the Unicode text. See the*^UNI* section on page 163 for the text format. '%LN<0-240>' = Set the lines of video being removed. *^BLN* section on page 149 for more information. '%EF<text effect name>' = Set the text effect. '%EC<text effect color>' = Set the text effect color. '%ML<max length>' = Set the maximum length of a text area. '%MK<input mask>' = Set the input mask of a text area. '%VL<0-1>' = Log-On/Log-Off the computer control connection '%VN<network name>' = Set network connection name. '%VP<password>' = Set the network connection password. Example: `SEND_COMMAND Panel,"'^BMF-500,1,%B10%CFRed%CB Blue %CTBlack%Ptest.png'"` Sets the button OFF state as well as the Border, Fill Color, Border Color, Text Color, and Bitmap.

"^" Button Commands (Cont.)	
^BMI Set the button mask image.	Mask image is used to crop a borderless button to a non-square shape. This is typically used with a bitmap. Syntax: `"'^BMI-<vt addr range>,<button states range>,<mask image>'"` Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). mask image = Graphic file used. Example: `SEND_COMMAND Panel,"'^BMI-530,1&2,newMac.png'"` Sets the button with variable text 530 ON/OFF state mask image to 'newmac.png'.
^BML Set the maximum length of the text area button.	If this value is set to zero (0) there is no max length. The maximum length available is 2000. This is only for a Text area input button and not for a Text area input masking button. Syntax: `"'^BML-<vt addr range>,<max length>'"` Variable: variable text address range = 1 - 4000. max length = 2000 (0=no max length). Example: `SEND_COMMAND Panel,"'^BML-500,20'"` Sets the maximum length of the text area input button to 20 characters.
^BMP Assign a picture to those buttons with a defined address range.	Syntax: `"'^BMP-<vt addr range>,<button states range>,<name of bitmap/ picture>'"` Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). name of bitmap/picture = 1 - 50 ASCII characters. Example: `SEND_COMMAND Panel,"'^BMP-500.504&510.515,1,bitmap.png'"` Sets the OFF state picture for the buttons with variable text ranges of 500-504 & 510-515.
^BNC Clear current TakeNote annotations.	Syntax: `"'^BNC-<vt addr range>,<command value>'"` Variable: variable text address range = 1 - 4000. command value = (0= clear, 1= clear all). Example: `SEND_COMMAND Panel,"'^BNC-973,0'"` Clears the annotation of the TakeNote button with variable text 973.
^BNN Set the TakeNote network name for the specified Addresses.	Syntax: `"'^BNN-<vt addr range>,<network name>'"` Variable: variable text address range = 1 - 4000. network name = Use a valid IP Address. Example: `SEND_COMMAND Panel,"'^BNN-973,192.168.169.99'"` Sets the TakeNote button network name to 192.168.169.99.

"^" Button Commands (Cont.)	
^BNP Set the TakeNote network password for the specified Addresses.	Syntax: `"'^BNP-<vt addr range>,<network password>'"` Variable: variable text address range = 1 - 4000. network password = Password for the network. Example: `SEND_COMMAND Panel,"'^BNN-973,12345'"` Sets the TakeNote button network password to 12345.
^BNT Set the TakeNote network port for the specified Addresses.	Syntax: `"'^BNT-<vt addr range>,<network port>'"` Variable: variable text address range = 1 - 4000. network port = 1 - 65535. Example: `SEND_COMMAND Panel,"'^BNT-973,5000'"` Sets the TakeNote button network port to 5000.
^BOP Set the button opacity.	The button opacity can be specified as a decimal between 0 - 255, where zero (0) is invisible and 255 is opaque, or as a HEX code, as used in the color commands by preceding the HEX code with the # sign. In this case, #00 becomes invisible and #FF becomes opaque. If the opacity is set to zero (0), this does not make the button inactive, only invisible. Syntax: `"'^BOP-<vt addr range>,<button states range>,<button opacity>'"` Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). button opacity = 0 (invisible) - 255 (opaque). Example: `SEND_COMMAND Panel,"'^BOP-500.504&510.515,1,200'"` Example 2: `SEND_COMMAND Panel,"'^BOP-500.504&510.515,1,#C8'"` Both examples set the opacity of the buttons with the variable text range of 500-504 and 510-515 to 200.

"^" Button Commands (Cont.)	
^BOR Set a border to a specific border style associated with a border value for those buttons with a defined address range.	Refer to theBorder Styles and Programming Numbers table on page 143 for more information. Syntax: `"'^BOR-<vt addr range>,<border style name or border value>'"` Variable: variable text address range = 1 - 4000. border style name = Refer to theBorder Styles and Programming Numbers table on page 143. border value = 0 - 41. Examples: `SEND_COMMAND Panel,"'^BOR-500.504&510.515,10'"` Sets the border by number (#10) to those buttons with the variable text range of 500-504 & 510-515. `SEND_COMMAND Panel,"'^BOR-500.504&510,AMX Elite -M'"` Sets the border by name (AMX Elite) to those buttons with the variable text range of 500-504 & 510-515. The border style is available through the TPDesign4 border-style drop-down list. Refer to theTPD4 Border Styles by Name table on page 143 for more information.
^BOS Set the button to display either a Video or Non-Video window.	Syntax: `"'^BOS-<vt addr range>,<button states range>,<video state>'"` Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). video state = Video Off = 0 and Video On = 1. Example: `SEND_COMMAND Panel,"'^BOS-500,1,1'"` Sets the button to display video.
^BPP Set or clear the protected page flip flag of a button.	Zero clears the flag. Syntax: `"'^BPP-<vt addr range>,<protected page flip flag value>'"` Variable: variable text address range = 1 - 4000. protected page flip flag value range = 0 - 4 (**0 clears the flag**). Example: `SEND_COMMAND Panel,"'^BPP-500,1'"` Sets the button to protected page flip flag 1 (sets it to password 1).
^BRD Set the border of a button state/ states.	**Only if** the specified border is not the same as the current border. The border names are available through the TPDesign4 border-name drop-down list. Syntax: `"'^BRD-<vt addr range>,<button states range>,<border name>'"` Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). border name = Refer toBorder Styles and Programming Numbers table on page 143. Example: `SEND_COMMAND Panel,"'^BRD-500.504&510.515,1&2,Quad Line'"` Sets the border by name (Quad Line) to those buttons with the variable text range of 500-504 & 510-515. Refer to theTPD4 Border Styles by Name table on page 143.

"^" Button Commands (Cont.)	
^BSF Set the focus to the text area.	***Note**: Select one button at a time (single variable text address). Do not assign a variable text address range to set focus to multiple buttons. Only one variable text address can be in focus at a time.* Syntax: `"'^BSF-<vt addr range>,<selection value>'"` Variable: variable text address range = 1 - 4000. selection value = Unselect = 0 and select = 1. Example: `SEND_COMMAND Panel,"'^BSF-500,1'"` Sets the focus to the text area of the button.
^BSM Submit text for text area buttons.	This command causes the text areas to send their text as strings to the NetLinx Master. Syntax: `"'^BSM-<vt addr range>'"` Variable: variable text address range = 1 - 4000. Example: `SEND_COMMAND Panel,"'^BSM-500'"` Submits the text of the text area button.
^BSO Set the sound played when a button is pressed.	If the sound name is blank the sound is then cleared. If the sound name is not matched, the button sound is not changed. Syntax: `"'^BSO-<vt addr range>,<button states range>,<sound name>'"` Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). sound name = (**blank** - sound cleared, **not matched** - button sound not changed). Example: `SEND_COMMAND Panel,"'^BSO-500,1&2,music.wav'"` Assigns the sound 'music.wav' to the button Off/On states.
^BSP Set the button size and position.	Set the button size and its position on the page. Syntax: `"'^BSP-<vt addr range>,<left>,<top>,<right>,<bottom>'"` Variable: variable text address range = 1 - 4000. left = left side of page. top = top of page. right = right side of page. bottom = bottom of page. Example: `SEND_COMMAND Panel,"'^BSP-530,left,top'"` Sets the button with variable text 530 in the left side top of page.

"^" Button Commands (Cont.)	
^BVL Log-On/Log-Off the computer control connection.	Syntax: "'^BVL-<vt addr range>,<connection>'" Variable: variable text address range = 1 - 4000. connection = 0 (Log-Off connection) and 1 (Log-On connection). Example: SEND_COMMAND Panel,"'^BVL-500,0'" Logs-off the computer control connection of the button.
^BVN Set the network name for the specified address.	Syntax: "'^BVN-<vt addr range>,<network name>'" Variable: variable text address range = 1 - 4000. network name = 1 - 50 ASCII characters. Example: SEND_COMMAND Panel,"'^BVN-500,191.191.191.191'" Sets the network name to '191.191.191.191' for the specific control button.
^BVP Set the network password for the specified address.	Syntax: "'^BVP-<vt addr range>,<network password>'" Variable: variable text address range = 1 - 4000. network password = 1 - 50 ASCII characters. Example: SEND_COMMAND Panel,"'^BVP-500,PCLOCK'" Sets the password to PCLOCK for the specific PC control button.
^BVT Set the computer control network port for the specified address.	Syntax: "'^BVT-<vt addr range>,<network port>'" Variable: variable text address range = 1 - 4000. network port = 1 - 65535. Example: SEND_COMMAND Panel,"'^BVT-500,5000'" Sets the network port to 5000.
^BWW Set the button word wrap feature to those buttons with a defined address range.	By default, word-wrap is Off. Syntax: "'^BWW-<vt addr range>,<button states range>,<word wrap>'" Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). word wrap = (0=Off and 1=On). Default is Off. Example: SEND_COMMAND Panel,"'^BWW-500,1,1'" Sets the word wrap on for the button's Off state.

"^" Button Commands (Cont.)	
^CPF Clear all page flips from a button.	Syntax: `"'^CPF-<vt addr range>'"` Variable: variable text address range = 1 - 4000. Example: `SEND_COMMAND Panel,"'^CPF-500'"` Clears all page flips from the button.
^DPF Delete page flips from button if it already exists.	Syntax: `"'^DFP-<vt addr range>,<actions>,<page name>'"` Variable: variable text address range = 1 - 4000. actions = **Stan**[dardPage] - Flip to standard page **Prev**[iousPage] - Flip to previous page **Show**[Popup] - Show Popup page **Hide**[Popup] - Hide Popup page **Togg**[lePopup] - Toggle popup state **ClearG**[roup] - Clear popup page group from all pages **ClearP**[age] - Clear all popup pages from a page with the pecified page name **ClearA**[ll] - Clear all popup pages from all pages page name = 1 - 50 ASCII characters. Example: `SEND COMMAND Panel,"'^DPF-409,Prev'"` Deletes the assignment of a button from flipping to a previous page.
^ENA Enable or disable buttons with a set variable text range.	Syntax: `"'^ENA-<vt addr range>,<command value>'"` Variable: variable text address range = 1 - 4000. command value = (0= disable, 1= enable) Example: `SEND_COMMAND Panel,"'^ENA-500.504&510.515,0'"` Disables button pushes on buttons with variable text range 500-504 & 510-515.
^FON Set a font to a specific Font ID value for those buttons with a defined address range.	Font ID numbers are generated by the TPDesign4 programmers report. Syntax: `"'^FON-<vt addr range>,<button states range>,<font value>'"` Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). font value = range = 1 - XXX. Refer to theDefault Font Styles and ID Numbers table on page 143. Example: `SEND_COMMAND Panel,"'^FON-500.504&510.515,1&2,4'"` Sets the font size to font ID #4 for the On and Off states of buttons with the variable text range of 500-504 & 510-515. ***Note**: The Font ID is generated by TPD4 and is located in TPD4 through the Main menu. Panel > Generate Programmer's Report >Text Only Format >Readme.txt.*

"^" Button Commands (Cont.)	
^GDI Change the bargraph drag increment.	Syntax: "'^GDI-<vt addr range>,<bargraph drag increment>'" Variable: variable text address range = 1 - 4000. bargraph drag increment = The default drag increment is 256. Example: SEND_COMMAND Panel,"'^GDI-7,128'" Sets the bargraph with variable text 7 to a drag increment of 128.
^GIV Invert the joystick axis to move the origin to another corner.	Parameters 1,2, and 3 will cause a bargraph or slider to be inverted regardless of orientation. Their effect will be as described for joysticks. Syntax: "'^GIV-<vt addr range>,<joystick axis to invert>'" Variable: variable text address range = 1 - 4000. joystick axis to invert = 0 - 3. 0 1 2 3 0 = Normal 1 = Invert horizontal axis 2 = Invert vertical axis 3 = Invert both axis locations For a bargraph 1 = Invert , 0 = Non Invert Example: SEND_COMMAND Panel,"'^GIV-500,3'" Inverts the joystick axis origin to the bottom right corner.
^GLH Change the bargraph upper limit.	Syntax: "'^GLH-<vt addr range>,<bargraph hi>'" Variable: variable text address range = 1 - 4000. bargraph limit range = 1 - 65535 (*bargraph upper limit range*). Example: SEND_COMMAND Panel,"'^GLH-500,1000'" Changes the bargraph upper limit to 1000.
^GLL Change the bargraph lower limit.	Syntax: "'^GLL-<vt addr range>,<bargraph low>'" Variable: variable text address range = 1 - 4000. bargraph limit range = 1 - 65535 (*bargraph lower limit range*). Example: SEND_COMMAND Panel,"'^GLL-500,150'" Changes the bargraph lower limit to 150.
^GRD Change the bargraph ramp-down time in 1/10th of a second.	Syntax: "'^GRD-<vt addr range>,<bargraph ramp down time>'" Variable: variable text address range = 1 - 4000. bargraph ramp down time = In 1/10th of a second intervals. Example: SEND_COMMAND Panel,"'^GRD-500,200'" Changes the bargraph ramp down time to 20 seconds.

<table>
<tr><th colspan="2">"^" Button Commands (Cont.)</th></tr>
<tr><td>^GRU
Change the bargraph ramp-up time in 1/10th of a second.</td><td>Syntax:
"'^GRU-<vt addr range>,<bargraph ramp up time>'"
Variable:
variable text address range = 1 - 4000.
bargraph ramp up time = In 1/10th of a second intervals.
Example:
SEND_COMMAND Panel,"'^GRU-500,100'"
Changes the bargraph ramp up time to 10 seconds.</td></tr>
<tr><td>^GSC
Change the bargraph slider color or joystick cursor color.</td><td>A user can also assign the color by Name and R,G,B value (RRGGBB or RRGGBBAA).
Syntax:
"'^GSC-<vt addr range>,<color value>'"
Variable:
variable text address range = 1 - 4000.
color value = Refer to theRGB Values for all 88 Basic Colors table on page 141.
Example:
SEND_COMMAND Panel,"'^GSC-500,12'"
Changes the bargraph or joystick slider color to Yellow.</td></tr>
<tr><td>^GSN
Change the bargraph slider name or joystick cursor name.</td><td>Slider names and cursor names can be found in the TPDesign4 slider name and cursor drop-down list.
Syntax:
"'^GSN-<vt addr range>,<bargraph slider name>'"
Variable:
variable text address range = 1 - 4000.
bargraph slider name = See table below.
<table><tr><td colspan="3">Bargraph Slider Names:</td></tr><tr><td>None</td><td>Ball</td><td>Circle -L</td></tr><tr><td>Circle -M</td><td>Circle -S</td><td>Precision</td></tr><tr><td>Rectangle -L</td><td>Rectangle -M</td><td>Rectangle -S</td></tr><tr><td>Windows</td><td>Windows Active</td><td></td></tr><tr><td colspan="3">Joystick Cursor Names:</td></tr><tr><td>None</td><td>Arrow</td><td>Ball</td></tr><tr><td>Circle</td><td>Crosshairs</td><td>Gunsight</td></tr><tr><td>Hand</td><td>Metal</td><td>Spiral</td></tr><tr><td>Target</td><td>View Finder</td><td></td></tr></table>Example:
SEND_COMMAND Panel,"'^GSN-500,Ball'"
Changes the bargraph slider name or the Joystick cursor name to 'Ball'.</td></tr>
</table>

<table>
<tr><th colspan="2">"^" Button Commands (Cont.)</th></tr>
<tr><td>^ICO
Set the icon to a button.</td><td>Syntax:
"'^ICO-<vt addr range>,<button states range>,<icon index>'"
Variable:
variable text address range = 1 - 4000.
button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
icon index range = 0 - 9900 (a value of 0 is clear).
Example:
SEND_COMMAND Panel,"'^ICO-500.504&510.515,1&2,1'"
Sets the icon for On and Off states for buttons with variable text ranges of 500-504 & 510-515.</td></tr>
<tr><td>^JSB
Set bitmap/ picture alignment using a numeric keypad layout for those buttons with a defined address range.</td><td>The alignment of 0 is followed by ',<left>,<top>'. The left and top coordinates are relative to the upper left corner of the button.
Syntax:
"'^JSB-<vt addr range>,<button states range>,<new text alignment>'"
Variable:
variable text address range = 1 - 4000.
button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
new text alignment = Value of 1- 9 corresponds to the following locations:
0
<table><tr><td>1</td><td>2</td><td>3</td></tr><tr><td>4</td><td>5</td><td>6</td></tr><tr><td>7</td><td>8</td><td>9</td></tr></table>Zero can be used for an absolute position
Example:
SEND_COMMAND Panel,"'^JSB-500.504&510.515,1&2,1'"
Sets the off/on state picture alignment to upper left corner for those buttons with variable text ranges of 500-504 & 510-515.</td></tr>
<tr><td>^JSI
Set icon alignment using a numeric keypad layout for those buttons with a defined address range.</td><td>The alignment of 0 is followed by ',<left>,<top>'. The left and top coordinates are relative to the upper left corner of the button.
Syntax:
"'^JSI-<vt addr range>,<button states range>,<new icon alignment>'"
Variable:
variable text address range = 1 - 4000.
button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
new icon alignment = Value of 1 - 9 corresponds to the following locations:
0
<table><tr><td>1</td><td>2</td><td>3</td></tr><tr><td>4</td><td>5</td><td>6</td></tr><tr><td>7</td><td>8</td><td>9</td></tr></table>Zero can be used for an absolute position
Example:
SEND_COMMAND Panel,"'^JSI-500.504&510.515,1&2,1'"
Sets the Off/On state icon alignment to upper left corner for those buttons with variable text range of 500-504 & 510-515.</td></tr>
</table>

<table>
<tr><th colspan="2">"^" Button Commands (Cont.)</th></tr>
<tr><td>^JST
Set text alignment using a numeric keypad layout for those buttons with a defined address range.</td><td>The alignment of 0 is followed by ',<left>,<top>'. The left and top coordinates are relative to the upper left corner of the button.
Syntax:
"'^JST-<vt addr range>,<button states range>,<new text alignment>'"
Variable:
variable text address range = 1 - 4000.
button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
new text alignment = Value of 1 - 9 corresponds to the following locations:
0
<table><tr><td>1</td><td>2</td><td>3</td></tr><tr><td>4</td><td>5</td><td>6</td></tr><tr><td>7</td><td>8</td><td>9</td></tr></table>Zero can be used for an absolute position
Example:
SEND_COMMAND Panel,"'^JST-500.504&510.515,1&2,1'"
Sets the text alignment to the upper left corner for those buttons with variable text ranges of 500-504 & 510-515.</td></tr>
<tr><td>^MBT
Set the Mouse Button mode On for the virtual PC.</td><td>Syntax:
"'^MBT-<pass data>'"
Variable:
pass data:
0 = None
1 = Left
2 = Right
3 = Middle
Example:
SEND COMMAND Panel,"'^MBT-1'"
Sets the mouse button mode to 'Left Mouse Click'.</td></tr>
<tr><td>^MDC
Turn On the 'Mouse double-click' feature for the virtual PC.</td><td>Syntax:
"'^MDC'"
Example:
SEND COMMAND Panel,"'^MDC'"
Sets the mouse double-click for use with the virtual PC.</td></tr>
<tr><td>^SHO
Show or hide a button with a set variable text range.</td><td>Syntax:
"'^SHO-<vt addr range>,<command value>'"
Variable:
variable text address range = 1 - 4000.
command value = (0= hide, 1= show).
Example:
SEND_COMMAND Panel,"'^SHO-500.504&510.515,0'"
Hides buttons with variable text address range 500-504 & 510-515.</td></tr>
</table>

"^" Button Commands (Cont.)	
^SKT Receive touch information on specified socket.	Syntax: `'^SKT-<0=disable socket, greater than 1023=enable socket on specified port>` Only socket values equal to or greater than 1024 are valid. The panel will open up a TCP listening socket on the port specified. User or 3rd party program can connect to the panel using this port/socket number and receive touch/release/move strings. By default, the panel disables touch notifications on startup. Format of the output is: <Press/Release/Move>,<x-coordinate>,<y-coordinate> Example: `send_command TP, '^SKT-7425' (enables touch notifications on socket 7425) send_command TP, '^SKT-0' (disable touch notification)`
^TEC Set the text effect color for the specified addresses/states to the specified color.	The Text Effect is specified by name and can be found in TPD4. You can also assign the color by name or RGB value (RRGGBB or RRGGBBAA). Syntax: `"'^TEC-<vt addr range>,<button states range>,<color value>'"` Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). color value = Refer to theRGB Values for all 88 Basic Colors table on page 141. Example: `SEND_COMMAND Panel,"'^TEC-500.504&510.515,1&2,12'"` Sets the text effect color to Very Light Yellow on buttons with variable text 500-504 and 510-515.
^TEF Set the text effect.	The Text Effect is specified by name and can be found in TPD4. Syntax: `"'^TEF-<vt addr range>,<button states range>,<text effect name>'"` Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). text effect name = **Refer to theText Effects table on page 163 for a listing of text effect names**. Example: `SEND_COMMAND Panel,"'^TEF-500.504&510.515,1&2,Soft Drop Shadow 3'"` Sets the text effect to Soft Drop Shadow 3 for the button with variable text range 500-504 and 510-515.
^TXT Assign a text string to those buttons with a defined address range.	Sets Non-Unicode text. Syntax: `"'^TXT-<vt addr range>,<button states range>,<new text>'"` Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). new text = 1 - 50 ASCII characters. Example: `SEND_COMMAND Panel,"'^TXT-500.504&510.515,1&2,Test Only'"` Sets the On and Off state text for buttons with the variable text ranges of 500-504 & 510-515.

"^" Button Commands (Cont.)	
^UNI Set Unicode text.	For the ^UNI command (%UN and ^BMF command), the Unicode text is sent as ASCII-HEX nibbles. Syntax: `"'^UNI-<vt addr range>,<button states range>,<unicode text>'"` Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). unicode text = Unicode HEX value. Example: `SEND_COMMAND Panel,"'^UNI-500,1,0041'"` Sets the button's unicode character to 'A'. ***Note:*** *To send the variable text 'A' in unicode to all states of the variable text button 1, (for which the character code is 0041 Hex), send the following command:* `SEND_COMMAND TP,"'^UNI-1,0,0041'"` Note: Unicode is always represented in a HEX value. TPD4 generates (through the Text Enter Box dialog) unicode HEX values. Refer to the TPDesign4 Instruction Manual for more information.

Text Effects Names

The following is a listing of text effects names (associated with the **^TEF** command on page 162).

Text Effects		
• Glow -S	• Medium Drop Shadow 1	• Hard Drop Shadow 1
• Glow -M	• Medium Drop Shadow 2	• Hard Drop Shadow 2
• Glow -L	• Medium Drop Shadow 3	• Hard Drop Shadow 3
• Glow -X	• Medium Drop Shadow 4	• Hard Drop Shadow 4
• Outline -S	• Medium Drop Shadow 5	• Hard Drop Shadow 5
• Outline -M	• Medium Drop Shadow 6	• Hard Drop Shadow 6
• Outline -L	• Medium Drop Shadow 7	• Hard Drop Shadow 7
• Outline -X	• Medium Drop Shadow 8	• Hard Drop Shadow 8
• Soft Drop Shadow 1	• Medium Drop Shadow 1 with outline	• Hard Drop Shadow 1 with outline
• Soft Drop Shadow 2	• Medium Drop Shadow 2 with outline	• Hard Drop Shadow 2 with outline
• Soft Drop Shadow 3	• Medium Drop Shadow 3 with outline	• Hard Drop Shadow 3 with outline
• Soft Drop Shadow 4	• Medium Drop Shadow 4 with outline	• Hard Drop Shadow 4 with outline
• Soft Drop Shadow 5	• Medium Drop Shadow 5 with outline	• Hard Drop Shadow 5 with outline
• Soft Drop Shadow 6	• Medium Drop Shadow 6 with outline	• Hard Drop Shadow 6 with outline
• Soft Drop Shadow 7	• Medium Drop Shadow 7 with outline	• Hard Drop Shadow 7 with outline
• Soft Drop Shadow 8	• Medium Drop Shadow 8 with outline	• Hard Drop Shadow 8 with outline
• Soft Drop Shadow 1 with outline		
• Soft Drop Shadow 2 with outline		
• Soft Drop Shadow 3 with outline		
• Soft Drop Shadow 4 with outline		
• Soft Drop Shadow 5 with outline		
• Soft Drop Shadow 6 with outline		
• Soft Drop Shadow 7 with outline		
• Soft Drop Shadow 8 with outline		

Button Query Commands

Button Query commands reply back with a custom event. There will be one custom event for each button/state combination. Each query is assigned a unique custom event type. **The following example is for debug purposes only:**

```
NetLinx Example: CUSTOM_EVENT[device, Address, Custom event type]
DEFINE_EVENT
CUSTOM_EVENT[TP,529,1001]      // Text
CUSTOM_EVENT[TP,529,1002]      // Bitmap
CUSTOM_EVENT[TP,529,1003]      // Icon
CUSTOM_EVENT[TP,529,1004]      // Text Justification
CUSTOM_EVENT[TP,529,1005]      // Bitmap Justification
CUSTOM_EVENT[TP,529,1006]      // Icon Justification
CUSTOM_EVENT[TP,529,1007]      // Font
CUSTOM_EVENT[TP,529,1008]      // Text Effect Name
CUSTOM_EVENT[TP,529,1009]      // Text Effect Color
CUSTOM_EVENT[TP,529,1010]      // Word Wrap
CUSTOM_EVENT[TP,529,1011]      // ON state Border Color
CUSTOM_EVENT[TP,529,1012]      // ON state Fill Color
CUSTOM_EVENT[TP,529,1013]      // ON state Text Color
CUSTOM_EVENT[TP,529,1014]      // Border Name
CUSTOM_EVENT[TP,529,1015]      // Opacity

{
   Send_String 0,"'ButtonGet Id=',ITOA(CUSTOM.ID),' Type=',ITOA(CUSTOM.TYPE)"
   Send_String 0,"'Flag   =',ITOA(CUSTOM.FLAG)"
   Send_String 0,"'VALUE1 =',ITOA(CUSTOM.VALUE1)"
   Send_String 0,"'VALUE2 =',ITOA(CUSTOM.VALUE2)"
   Send_String 0,"'VALUE3 =',ITOA(CUSTOM.VALUE3)"
   Send_String 0,"'TEXT   =',CUSTOM.TEXT"
   Send_String 0,"'TEXT LENGTH =',ITOA(LENGTH_STRING(CUSTOM.TEXT))"
}
```

All custom events have the following 6 fields:

Custom Event Fields	
Field	**Description**
Uint Flag	0 means text is a standard string, 1 means Unicode encoded string
slong value1	button state number
slong value2	actual length of string (this is not encoded size)
slong value3	index of first character (usually 1 or same as optional index
string text	the text from the button
text length (string encode)	button text length

These fields are populated differently for each query command. The text length (String Encode) field is not used in any command.

Button Query Commands	
?BCB Get the current border color.	Syntax: `"'?BCB-<vt addr range>,<button states range>'"` Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). custom event type **1011:** Flag - zero Value1 - Button state number Value2 - Actual length of string (should be 9) Value3 - Zero Text - Hex encoded color value (ex: #000000FF) Text length - Color name length (should be 9) Example: `SEND COMMAND Panel,"'?BCB-529,1'"` Gets the button 'OFF state' border color. information. The result sent to the Master would be: `ButtonGet Id = 529 Type = 1011` `Flag = 0` `VALUE1 = 1` `VALUE2 = 9` `VALUE3 = 0` `TEXT = #222222FF` `TEXT LENGTH = 9`
?BCF Get the current fill color.	Syntax: `"'?BCF-<vt addr range>,<button states range>'"` Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). custom event type **1012:** Flag - Zero Value1 - Button state number Value2 - Actual length of string (should be 9) Value3 - Zero Text - Hex encoded color value (ex: #000000FF) Text length - Color name length (should be 9) Example: `SEND COMMAND Panel,"'?BCF-529,1'"` Gets the button 'OFF state' fill color information. The result sent to the Master would be: `ButtonGet Id = 529 Type = 1012` `Flag = 0` `VALUE1 = 1` `VALUE2 = 9` `VALUE3 = 0` `TEXT = #FF8000FF` `TEXT LENGTH = 9`

Button Query Commands (Cont.)	
?BCT Get the current text color.	Syntax: "'?BCT-<vt addr range>,<button states range>'" Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). custom event type **1013:** Flag - Zero Value1 - Button state number Value2 - Actual length of string (should be 9) Value3 - Zero Text - Hex encoded color value (ex: #000000FF) Text length - Color name length (should be 9) Example: SEND COMMAND Panel,"'?BCT-529,1'" Gets the button 'OFF state' text color information. The result sent to Master would be: ButtonGet Id = 529 Type = 1013 Flag = 0 VALUE1 = 1 VALUE2 = 9 VALUE3 = 0 TEXT = #FFFFFEFF TEXT LENGTH = 9
?BMP Get the current bitmap name.	Syntax: "'?BMP-<vt addr range>,<button states range>'" Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). custom event type **1002:** Flag - Zero Value1 - Button state number Value2 - Actual length of string Value3 - Zero Text - String that represents the bitmap name Text length - Bitmap name text length (should be 9) Example: SEND COMMAND Panel,"'?BMP-529,1'" Gets the button 'OFF state' bitmap information. The result sent to the Master would be: ButtonGet Id = 529 Type = 1002 Flag = 0 VALUE1 = 1 VALUE2 = 9 VALUE3 = 0 TEXT = Buggs.png TEXT LENGTH = 9

Button Query Commands (Cont.)	
?BOP Get the overall button opacity.	Syntax: `"'?BOP-<vt addr range>,<button states range>'"` Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). custom event type **1015:** Flag - Zero Value1 - Button state number Value2 - Opacity Value3 - Zero Text - Blank Text length - Zero Example: `SEND COMMAND Panel,"'?BOP-529,1'"` Gets the button 'OFF state' opacity information. The result sent to the Master would be: `ButtonGet Id = 529 Type = 1015` `Flag = 0` `VALUE1 = 1` `VALUE2 = 200` `VALUE3 = 0` `TEXT =` `TEXT LENGTH = 0`
?BRD Get the current border name.	Syntax: `"'?BRD-<vt addr range>,<button states range>'"` Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). custom event type **1014:** Flag - Zero Value1 - Button state number Value2 - Actual length of string Value3 - Zero Text - String that represents border name Text length - Border name length Example: `SEND COMMAND Panel,"'?BRD-529,1'"` Gets the button 'OFF state' border information. The result sent to the Master would be: `ButtonGet Id = 529 Type = 1014` `Flag = 0` `VALUE1 = 1` `VALUE2 = 22` `VALUE3 = 0` `TEXT = Double Bevel Raised -L` `TEXT LENGTH = 22`

Button Query Commands (Cont.)	
?BWW Get the current word wrap flag status.	Syntax: `"'?BWW-<vt addr range>,<button states range>'"` Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). custom event type **1010:** Flag - Zero Value1 - Button state number Value2 - 0 = no word wrap, 1 = word wrap Value3 - Zero Text - Blank Text length - Zero Example: `SEND COMMAND Panel,"'?BWW-529,1'"` Gets the button 'OFF state' word wrap flag status information. The result sent to the Master would be: `ButtonGet Id = 529 Type = 1010` `Flag = 0` `VALUE1 = 1` `VALUE2 = 1` `VALUE3 = 0` `TEXT =` `TEXT LENGTH = 0`
?FON Get the current font index.	Syntax: `"'?FON-<vt addr range>,<button states range>'"` Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). custom event type **1007:** Flag - Zero Value1 - Button state number Value2 - Font index Value3 - Zero Text - Blank Text length - Zero Example: `SEND COMMAND Panel,"'?FON-529,1'"` Gets the button 'OFF state' font type index information. The result sent to the Master would be: `ButtonGet Id = 529 Type = 1007` `Flag = 0` `VALUE1 = 1` `VALUE2 = 72` `VALUE3 = 0` `TEXT =` `TEXT LENGTH = 0`

Button Query Commands (Cont.)	
?ICO Get the current icon index.	Syntax: `"'?ICO-<vt addr range>,<button states range>'"` Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). custom event type **1003:** Flag - Zero Value1 - Button state number Value2 - Icon Index Value3 - Zero Text - Blank Text length - Zero Example: `SEND COMMAND Panel,"'?ICO-529,1&2'"` Gets the button 'OFF state' icon index information. The result sent to the Master would be: `ButtonGet Id = 529 Type = 1003` `Flag = 0` `VALUE1 = 2` `VALUE2 = 12` `VALUE3 = 0` `TEXT =` `TEXT LENGTH = 0`
?JSB Get the current bitmap justification.	Syntax: `"'?JSB-<vt addr range>,<button states range>'"` Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). custom event type **1005:** Flag - Zero Value1 - Button state number Value2 - 1 - 9 justify Value3 - Zero Text - Blank Text length - Zero Example: `SEND COMMAND Panel,"'?JSB-529,1'"` Gets the button 'OFF state' bitmap justification information. The result sent to the Master would be: `ButtonGet Id = 529 Type = 1005` `Flag = 0` `VALUE1 = 1` `VALUE2 = 5` `VALUE3 = 0` `TEXT =` `TEXT LENGTH = 0`

Button Query Commands (Cont.)	
?JSI Get the current icon justification.	Syntax: `"'?JSI-<vt addr range>,<button states range>'"` Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). custom event type **1006:** Flag - Zero Value1 - Button state number Value2 - 1 - 9 justify Value3 - Zero Text - Blank Text length - Zero Example: `SEND COMMAND Panel,"'?JSI-529,1'"` Gets the button 'OFF state' icon justification information. The result sent to the Master would be: `ButtonGet Id = 529 Type = 1006` `Flag = 0` `VALUE1 = 1` `VALUE2 = 6` `VALUE3 = 0` `TEXT =` `TEXT LENGTH = 0`
?JST Get the current text justification.	Syntax: `"'?JST-<vt addr range>,<button states range>'"` Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). custom event type **1004:** Flag - Zero Value1 - Button state number Value2 - 1 - 9 justify Value3 - Zero Text - Blank Text length - Zero Example: `SEND COMMAND Panel,"'?JST-529,1'"` Gets the button 'OFF state' text justification information. The result sent to the Master would be: `ButtonGet Id = 529 Type = 1004` `Flag = 0` `VALUE1 = 1` `VALUE2 = 1` `VALUE3 = 0` `TEXT =` `TEXT LENGTH = 0`

Button Query Commands (Cont.)	
?TEC Get the current text effect color.	Syntax: `"'?TEC-<vt addr range>,<button states range>'"` Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). custom event type **1009:** Flag - Zero Value1 - Button state number Value2 - Actual length of string (should be 9) Value3 - Zero Text - Hex encoded color value (ex: #000000FF) Text length - Color name length (should be 9) Example: `SEND COMMAND Panel,"'?TEC-529,1'"` Gets the button 'OFF state' text effect color information. The result sent to the Master would be: `ButtonGet Id = 529 Type = 1009` `Flag = 0` `VALUE1 = 1` `VALUE2 = 9` `VALUE3 = 0` `TEXT = #5088F2AE` `TEXT LENGTH = 9`
?TEF Get the current text effect name.	Syntax: `"'?TEF-<vt addr range>,<button states range>'"` Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). custom event type **1008:** Flag - Zero Value1 - Button state number Value2 - Actual length of string Value3 - Zero Text - String that represents the text effect name Text length - Text effect name length Example: `SEND COMMAND Panel,"'?TEF-529,1'"` Gets the button 'OFF state' text effect name information. The result sent to the Master would be: `ButtonGet Id = 529 Type = 1008` `Flag = 0` `VALUE1 = 1` `VALUE2 = 18` `VALUE3 = 0` `TEXT = Hard Drop Shadow 3` `TEXT LENGTH = 18`

Button Query Commands (Cont.)	
?TXT Get the current text information.	Syntax: `"'?TXT-<vt addr range>,<button states range>,<optional index>'"` Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). optional index = This is used if a string was too long to get back in one command. The reply will start at this index. custom event type **1001:** Flag - Zero Value1 - Button state number Value2 - Actual length of string Value3 - Index Text - Text from the button Text length - Button text length Example: `SEND COMMAND Panel,"'?TXT-529,1'"` Gets the button 'OFF state' text information. The result sent to the Master would be: `ButtonGet Id = 529 Type = 1001` `Flag = 0` `VALUE1 = 1` `VALUE2 = 14` `VALUE3 = 1` `TEXT = This is a test` `TEXT LENGTH = 14`

Panel Runtime Operations

Serial Commands are used in the AxcessX Terminal Emulator mode. These commands are case insensitive.

Panel Runtime Operation Commands	
ABEEP Output a single beep even if beep is Off.	Syntax: `"'ABEEP'"` Example: `SEND COMMAND Panel,"'ABEEP'"` Outputs a beep of duration 1 beep even if beep is Off.
ADBEEP Output a double beep even if beep is Off.	Syntax: `"'ADBEEP'"` Example: `SEND COMMAND Panel,"'ADBEEP'"` Outputs a double beep even if beep is Off.

Panel Runtime Operation Commands (Cont.)	
@AKB Pop up the keyboard icon and initialize the text string to that specified.	Keyboard string is set to null on power up and is stored until power is lost. The Prompt Text is optional. Syntax: `"'@AKB-<initial text>;<prompt text>'"` Variables: `initial text = 1 - 50 ASCII characters.` `prompt text = 1 - 50 ASCII characters.` Example: `SEND COMMAND Panel,"'@AKB-Texas;Enter State'"` Pops up the Keyboard and initializes the text string 'Texas' with prompt text 'Enter State'.
AKEYB Pop up the keyboard icon and initialize the text string to that specified.	Keyboard string is set to null on power up and is stored until power is lost. Syntax: `"'AKEYB-<initial text>'"` Variables: `initial text = 1 - 50 ASCII characters.` Example: `SEND COMMAND Panel,"'AKEYB-This is a Test'"` Pops up the Keyboard and initializes the text string 'This is a Test'.
AKEYP Pop up the keypad icon and initialize the text string to that specified.	The keypad string is set to null on power up and is stored until power is lost. Syntax: `"'AKEYP-<number string>'"` Variables: `number string = 0 - 9999.` Example: `SEND COMMAND Panel,"'AKEP-12345'"` Pops up the Keypad and initializes the text string '12345'.
AKEYR Remove the Keyboard/ Keypad.	Remove keyboard or keypad that was displayed using 'AKEYB', 'AKEYP', 'PKEYP', @AKB, @AKP, @PKP, @EKP, or @TKP commands. Syntax: `"'AKEYR'"` Example: `SEND COMMAND Panel,"'AKEYR'"` Removes the Keyboard/Keypad.
@AKP Pop up the keypad icon and initialize the text string to that specified.	Keypad string is set to null on power up and is stored until power is lost. The Prompt Text is optional. Syntax: `"'@AKP-<initial text>;<prompt text>'"` Variables: `initial text = 1 - 50 ASCII characters.` `prompt text = 1 - 50 ASCII characters.` Example: `SEND COMMAND Panel,"'@AKP-12345678;ENTER PASSWORD'"` Pops up the Keypad and initializes the text string '12345678' with prompt text 'ENTER PASSWORD'.

Panel Runtime Operation Commands (Cont.)	
@AKR Remove the Keyboard/ Keypad.	Remove keyboard or keypad that was displayed using 'AKEYB', 'AKEYP', 'PKEYP', @AKB, @AKP, @PKP, @EKP, or @TKP commands. Syntax: `"'@AKR'"` Example: `SEND COMMAND Panel,"'@AKR'"` Removes the Keyboard/Keypad.
BEEP Output a beep.	Syntax: `"'BEEP'"` Example: `SEND COMMAND Panel,"'BEEP'"` Outputs a beep.
BRIT Set the panel brightness.	Syntax: `"'BRIT-<brightness level>'"` Variable: brightness level = 0 - 100. Example: `SEND COMMAND Panel,"'BRIT-50'"` Sets the brightness level to 50.
@BRT Set the panel brightness.	Syntax: `"'@BRT-<brightness level>'"` Variable: brightness level = 0 - 100. Example: `SEND COMMAND Panel,"'@BRT-70'"` Sets the brightness level to 70.
DBEEP Output a double beep.	Syntax: `"'DBEEP'"` Example: `SEND COMMAND Panel,"'DBEEP'"` Outputs a double beep.
@EKP Extend the Keypad.	Pops up the keypad icon and initializes the text string to that specified. The Prompt Text is optional. Syntax: `"'@EKP-<initial text>;<prompt text>'"` Variables: `initial text = 1 - 50 ASCII characters.` `prompt text = 1 - 50 ASCII characters.` Example: `SEND COMMAND Panel,"'@EKP-33333333;Enter Password'"` Pops up the Keypad and initializes the text string '33333333' with prompt text 'Enter Password'.

Panel Runtime Operation Commands (Cont.)	
PKEYP Present a private keypad.	Pops up the keypad icon and initializes the text string to that specified. Keypad displays a '*' instead of the numbers typed. The Prompt Text is optional. Syntax: `"'PKEYP-<initial text>'"` Variables: `initial text = 1 - 50 ASCII characters.` Example: `SEND COMMAND Panel,"'PKEYP-123456789'"` Pops up the Keypad and initializes the text string '123456789' in '*'.
@PKP Present a private keypad.	Pops up the keypad icon and initializes the text string to that specified. Keypad displays a '*' instead of the numbers typed. The Prompt Text is optional. Syntax: `"'@PKP-<initial text>;<prompt text>'"` Variables: `initial text = 1 - 50 ASCII characters.` `prompt text = 1 - 50 ASCII characters.` Example: `SEND COMMAND Panel,"'@PKP-1234567;ENTER PASSWORD'"` Pops up the Keypad and initializes the text string 'ENTER PASSWORD' in '*'.
SETUP Send panel to SETUP page.	Syntax: `"'SETUP'"` Example: `SEND COMMAND Panel,"'SETUP'"` Sends the panel to the Setup Page.
SHUTDOWN Shut down the batteries providing power to the panel.	Syntax: `"'SHUTDOWN'"` Example: `SEND COMMAND Panel,"'SHUTDOWN'"` Shuts-down the batteries feeding power to the panel. This function saves the battery from discharging.
SLEEP Force the panel into screen saver mode.	Syntax: `"'SLEEP'"` Example: `SEND COMMAND Panel,"'SLEEP'"` Forces the panel into screen saver mode.
@SOU Play a sound file.	Syntax: `"'@SOU-<sound name>'"` Variables: `sound name = Name of the sound file. Supported sound file formats are: WAV & MP3.` Example: `SEND COMMAND Panel,"'@SOU-Music.wav'"` Plays the 'Music.wav' file.

Panel Runtime Operation Commands (Cont.)	
@SSL Change Sleep string.	Syntax: `"'@SSL-<string>'"` Variables: `string = name of sleep string.` Example: `SEND COMMAND Panel,"'@SWK-SLEEPNOW'"` Changes the sleep string to SLEEPNOW.
@SST Change Startup string.	Syntax: `"'@SST-<string>'"` Variables: `string = name of startup string.` Example: `SEND COMMAND Panel,"'@SWK-STARTUPNOW'"` Changes the startup string to STARTUPNOW.
@SWK Change Wakeup string.	Syntax: `"'@SWK-<string>'"` Variables: `string = name of wakeup string.` Example: `SEND COMMAND Panel,"'@SWK-WAKEUPNOW'"` Changes the wakeup string to WAKEUPNOW.
@TKP Present a telephone keypad.	Pops up the keypad icon and initializes the text string to that specified. The Prompt Text is optional. Syntax: `"'@TKP-<initial text>;<prompt text>'"` Variables: `initial text = 1 - 50 ASCII characters.` `prompt text = 1 - 50 ASCII characters.` Example: `SEND COMMAND Panel,"'@TKP-999.222.1211;Enter Phone Number'"` Pops-up the Keypad and initializes the text string '999.222.1211' with prompt text 'Enter Phone Number'.
^TNC Clears task note.	Syntax: `"'^TNC'"` Example: `SEND COMMAND Panel,"'^TNC'"` Clears task note.
TPAGEON Turn On page tracking.	This command turns On page tracking, whereby when the page or popups change, a string is sent to the Master. This string may be captured with a CREATE_BUFFER command for one panel and sent directly to another panel. Syntax: `"'TPAGEON'"` Example: `SEND COMMAND Panel,"'TPAGEON'"` Turns On page tracking.

Panel Runtime Operation Commands (Cont.)	
TPAGEOFF Turn Off page tracking.	Syntax: `"'TPAGEOFF'"` Example: `SEND COMMAND Panel,"'TPAGEOFF'"` Turns Off page tracking.
@VKB Popup the virtual keyboard.	Syntax: `"'@VKB'"` Example: `SEND COMMAND Panel,"'@VKB'"` Pops-up the virtual keyboard.
WAKE Force the panel out of screen saver mode.	Syntax: `"'WAKE'"` Example: `SEND COMMAND Panel,"'WAKE'"` Forces the panel out of the screen saver mode.

Input Commands

These Send Commands are case insensitive.

Input Commands	
^CAL Put panel in calibration mode.	Syntax: `"'^CAL'"` Example: `SEND COMMAND Panel,"'^CAL'"` Puts the panel in calibration mode.
^KPS Set the keyboard passthru.	Syntax: `"'^KPS-<pass data>'"` Variable: **pass data**: <blank/empty> = Disables the keyboard. 0 = Pass data to G4 application (default). This can be used with VPC or text areas. 1 - 4 = Not used. 5 = Sends out data to the Master. Example: `SEND COMMAND Panel,"'^KPS-5'"` Sets the keyboard passthru to the Master. Option 5 sends keystrokes directly to the Master via the Send Output String mechanism. This process sends a virtual keystroke command (^VKS) to the Master. Example 2: `SEND COMMAND Panel,"'^KPS-0'"` Disables the keyboard passthru to the Master. The following point defines how the parameters within this command work: • Accepts keystrokes from any of these sources: attached USB keyboard or Virtual keyboard.

Input Commands (Cont.)	
^MBT Set the mouse button mode for the virtual PC.	Syntax: `"'^MBT-<0-3>'"` Variable: 0 = None. 1 = Left. 2 = Middle. 3 = Right. Example: `SEND COMMAND Panel,"'^MBT-1'"` Sets the mouse button mode for the virtual PC to LEFT.
^MDC Set the mouse double click ON for the virtual PC.	Syntax: `"'^MDC'"` Example: `SEND COMMAND Panel,"'^MDC'"` Enables the double click for the virtual PC.
^MPS Set mouse pass through. Allows mouse input to multiple destinations simultaneously. Destinations are comma delimited.	Syntax: `"'^MPS-<0-6>,<0-6>,...'"` Variable: 0 = Pass mouse input to G4 application. 1-4 = Pass mouse input data to a VGA card with USP output for redirection to a computer. 5 = Pass mouse buttons to the NetLinx master in the form of a custom event. 6 = Pass mouse buttons and movement to the NetLinx master in the form of custom events. Example: `SEND COMMAND Panel,"'^MPS-0'"` Passes the mouse input to a connected G4 application. ***Note:*** *This command causes all mice connected to the G4 product and any mice on a computer connected via a VGA card with USB output to reset to position 0,0.*
^TPS TPI only. Set touch pass through.	Syntax: `"'^TPS-<0-1>'"` Variable: 1 = Creates a transparent connection between the touch input serial port and the program port. This is useful for connecting a PC to the program port and controlling touch input on that PC from the touch panel connected to the touch input port. This will cause the command terminal on the program port to shutdown. 0 = Undoes the changes. Example: `SEND COMMAND Panel,"'^TPS-1'"` Enables the touch pass through.
^VKS Send one or more virtual key strokes to the G4 application.	Key presses and key releases are not distinguished except in the case of CTRL, ALT, and SHIFT. **Refer to theEmbedded Codes table on page 179** that define special characters which can be included with the string but may not be represented by the ASCII character set. Syntax: `"'^VKS-<string>'"` Variable: string = Only 1 string per command/only one stroke per command. Example: `SEND COMMAND Panel,"'^VKS-'8"` Sends out the keystroke 'backspace' to the G4 application.

Embedded Codes

The following is a list of G4 compatible embedded codes:

Embedded Codes		
Decimal numbers	**Hexidecimal values**	**Virtual keystroke**
8	($08)	Backspace
13	($0D)	Enter
27	($1B)	ESC
128	($80)	CTRL key down
129	($81)	ALT key down
130	($82)	Shift key down
131	($83)	F1
132	($84)	F2
133	($85)	F3
134	($86)	F4
135	($87)	F5
136	($88)	F6
137	($89)	F7
138	($8A)	F8
139	($8B)	F9
140	($8C)	F10
141	($8D)	F11
142	($8E)	F12
143	($8F)	Num Lock
144	($90)	Caps Lock
145	($91)	Insert
146	($92)	Delete
147	($93)	Home
148	($94)	End
149	($95)	Page Up
150	($96)	Page Down
151	($97)	Scroll Lock
152	($98)	Pause
153	($99)	Break
154	($9A)	Print Screen
155	($9B)	SYSRQ
156	($9C)	Tab
157	($9D)	Windows
158	($9E)	Menu
159	($9F)	Up Arrow
160	($A0)	Down Arrow
161	($A1)	Left Arrow
162	($A2)	Right Arrow
192	($C0)	CTRL key up
193	($C1)	ALT key up
194	($C2)	Shift key up

Panel Setup Commands

These commands are case insensitive.

Panel Setup Commands	
CLOCK Sets the time and date on the panel.	Syntax: "'CLOCK mm-dd-yy hh:mm:ss'" Variables: mm = Month dd = Day yy = Year hh = Hour mm = Minute ss = Second Example: SEND_COMMAND Panel, "'CLOCK 04-19-76 19:16:00'" Sets the time and date on the panel to April 19, 1976, 7:16 PM.
^CFE Enable or disable the image Flash backup cache	Syntax: "'^CFE-<0/1>'" Variables: 0 - for disable 1 - for enable Example: SEND_COMMAND Panel, "'^CFE-1'" Tells the cache manager to enable the Flash backup image cache.
^CPR Purge the cache when needed in the context of the running program.	Syntax: "'^CPR-<cache mask>'" Variables: cache mask: • 0x0001 - Purge non-volatile (Flash) image cache • 0x0002 - Purge RAM image cache • 0x0003 - Purge both non-volatile and RAM image caches Example: SEND_COMMAND Panel, "'^CPR-3'" Purges all images from both primary RAM cache and backup Flash cache.
^CFS Modifies the size of the backup image Flash cache.	Syntax: "'^CFS-<size in MB>'" Variable: size in MB - MB of allocated Flash memory Example: SEND_COMMAND Panel, "'^CFS-12'" Modifies the Flash cache size to 12MB. The space is not immediately allocated to the backup cache, it is consumed as needed for new entries in the Flash cache. If the size is reduced to something less than the size of the items currently stored in Flash cache, the least recently used items are deleted one by one until the used disk space is less than the maximum provided in the ^CFS command. If the size is larger than the maximum size allowed for the Flash cache (determined by taking 75% of free Flash space), the size reverts to the maximum size allowed.

Panel Setup Commands (Cont.)	
^CFSM Sets the Flash cache to the maximum available size allowed for backup Flash cache. (determined by taking 75% of free Flash space)	Syntax: "'^CFSM'" Variable: There is no parameter for this command. Example: SEND_COMMAND Panel, "'^CFSM'" Modifies the Flash cache size to the maximum available size for the device.
^CEX Changes the default expiration time for entries in the image cache (applies to both primary RAM cache and backup Flash cache). The default expiration time applies to dynamic images only.	Syntax: "'^CEX-<time index>'" Variable: time index: • 1 = 2 Hours • 2 = 8 Hours • 3 = 1 Day • 4 = 2 Days • 5 = 5 Days • 0 = NEVER Example: SEND_COMMAND Panel, "'^CEX-4'" Changes the default expiration time to 2 Days.
^DLD Set the disable cradle LED flag.	Syntax: "'^DLD-<0/1>'" Variables: 0 - LEDs operate normally 1 - Cradle LEDs operate dim setting only Example: SEND_COMMAND Panel, "'^DLD-1'" Sets the cradle LEDs to the dim setting.
@PWD Set the page flip password.	@PWD sets the level 1 password only. Syntax: "'@PWD-<page flip password>'" Variables: page flip password = 1 - 50 ASCII characters. Example: SEND COMMAND Panel,"'@PWD-Main'" Sets the page flip password to 'Main'.
^PWD Set the page flip password.	Password level is required and must be 1 - 4. Syntax: "'^PWD-<password level>,<page flip password>'" Variables: password level = 1 - 4. page flip password = 1 - 50 ASCII characters. Example: SEND COMMAND Panel,"'^PWD-1,Main'" Sets the page flip password on Password Level 1 to 'Main'.

Panel Setup Commands (Cont.)	
@RPP Reset the protected password.	@RPP resets the protected password to its default (1988). Syntax: `"'@RPP'"` Example: `SEND COMMAND Panel,"'@RPP'"` Resets the protected Setup page password to '1988'.

Dynamic Image Commands

The following table describes Dynamic Image Commands.

Dynamic Image Commands	
^BBR Set the bitmap of a button to use a particular resource.	Syntax: `"'^BBR-<vt addr range>,<button states range>,<resource name>'"` Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). resource name = 1 - 50 ASCII characters. Example: `SEND_COMMAND Panel,"'^BBR-700,1,Sports_Image'"` Sets the resource name of the button to 'Sports_Image'.
^RAF Add new resources.	Adds any and all resource parameters by sending embedded codes and data. Since the embedded codes are preceded by a '%' character, any '%' character contained in the URL must be escaped with a second '%' character (see example). The file name field (indicated by a **%F** embedded code) may contain special escape sequences as shown in the *^RAF, ^RMF - Embedded Codes* table below. Syntax: `"'^RAF-<resource name>,<data>'"` Variables: • resource name = 1 - 50 ASCII characters. • data = Refers to the embedded codes, see the *^RAF, ^RMF - Embedded Codes* section on page 183. Example: `SEND_COMMAND Panel,"'^RAF-New Image,%P0%HAMX.COM%ALab/ Test%%5Ffile%Ftest.jpg'"` Adds a new resource. • The resource name is 'New Image' • %P (protocol) is an HTTP • %H (host name) is ***AMX.COM*** • %A (file path) is ***Lab/Test_file*** • %F (file name) is ***test.jpg***. Note that the **%%5F** in the file path is actually encoded as **%5F**.
^RFR Force a refresh for a given resource.	Syntax: `"'^RFR-<resource name>'"` Variable: resource name = 1 - 50 ASCII characters. Example: `SEND_COMMAND Panel,"'^RFR-Sports_Image'"` Forces a refresh on 'Sports_Image'.

Dynamic Image Commands (Cont.)	
^RMF Modify an existing resource.	Modifies any and all resource parameters by sending embedded codes and data. Since the embedded codes are preceded by a '%' character, any '%' character contained in the URL must be escaped with a second '%' character (see example). The file name field (indicated by a **%F** embedded code) may contain special escape sequences as shown in the *^RAF, ^RMF - Embedded Codes* section on page 183. Syntax: `"'^RMF-<resource name>,<data>'"` Variables: • resource name = 1 - 50 ASCII characters • data = Refers to the embedded codes, see the *^RAF, ^RMF - Embedded Codes* section on page 183. Example: `SEND_COMMAND Panel,"'^RMF-Sports_Image,%ALab%%5FTest/Images%Ftest.jpg'"` Changes the resource 'Sports_Image' file name to 'test.jpg' and the path to 'Lab_Test/Images'. Note that the **%%5F** in the file path is actually encoded as **%5F**.
^RSR Change the refresh rate for a given resource.	Syntax: `"'^RSR-<resource name>,<refresh rate>'"` Variable: resource name = 1 - 50 ASCII characters. refresh rate = Measured in seconds. Example: `SEND_COMMAND Panel,"'^RSR-Sports_Image,5'"` Sets the refresh rate to 5 seconds for the given resource ('Sports_Image').

^RAF, ^RMF - Embedded Codes

The ^RAF and ^RMF commands add and modify any and all resource parameters by sending embedded codes and data:

```
"'^RAF-<resource name>,<data>'"
"'^RMF-<resource name>,<data>'"
```

The <data> variable uses the embedded codes described in the following table:

^RAF, ^RMF - Embedded Codes		
Parameter	Embedded Code	Description
protocol	'%P <0-1>'	Set protocol. HTTP (0) or FTP (1).
user	'%U <user>'	Set Username for authentication.
password	'%S <password>'	Set Password for authentication.
host	'%H <host>'	Set Host Name (fully qualified DNS or IP Address).
file	'%F <file>'	Full path to the location of the file or program that will return the resource. The path must be a valid HTTP URL minus the protocol and host. The only exception to this is the inclusion of special escape sequences and in the case of FTP protocol, regular expressions.
path	'%A <path>'	Set Directory path. The path must be a valid HTTP URL minus the protocol, host and filename. The only exception to this is the inclusion of special escape sequences and in the case of FTP protocol, regular expressions.

^RAF, ^RMF - Embedded Codes (Cont.)		
Parameter	Embedded Code	Description
refresh	'%R <refresh 1-65535>'	The number of seconds between refreshes in which the resource is downloaded again. Refreshing a resource causes the button displaying that resource to refresh also. The default value is 0 (only download the resource once).
newest	'%N <0-1>'	Set the newest file. A value of 1 means that only the most recent file matching the pattern is downloaded. ***Note**: The 'newest file' option only applies to FTP Dynamic Images, and only those that have pattern matching as part of their filename. Neither 'newest file' nor pattern matching apply to HTTP Dynamic Images.* *When set, the panel will first pull a list of files matching the given pattern from the specified FTP server and path. The timestamps of the items in the list will be compared, with the newest one being displayed on the panel. This is useful for source devices that place a uniquely named still image in a folder at constant intervals, allowing the panel always to display the most recent one.*
preserve	'%V <0-1>'	Set the value of the preserve flag. Default is 0. Currently preserve has no function.

Escape Sequences

The ^RAF and ^RMF commands support the replacement of any special escape sequences in the filename (specified by the **%F** embedded code) with the corresponding data obtained from the system as outlined in the table below:

Escape Sequences	
Sequence	Panel Information
$DV	Device Number
$SY	System Number
$IP	IP Address
$HN	Host Name
$MC	Mac Address
$ID	Neuron ID (*Only supported on panels that use ICSNet; ignored on all other panels*)
$PX	X resolution of current panel mode/file
$PY	Y resolution of current panel mode/file
$ST	Current state
$AC	Address code
$AP	Address port
$CC	Channel code
$CP	Channel port
$LC	Level code
$LP	Level port
$BX	X Resolution of Current button
$BY	Y Resolution of Current button
$BN	Name of Button

For instance, **http://www.amx.com/img.asp?device=$DV**

would become

http://www.amx.com/img.asp?device=10001.

Intercom Commands

The following is a listing and descriptions of panel intercom commands.

Intercom Commands	
^ICE Ends an intercom call.	Syntax: `"'^ICE'"` Example: `SEND_COMMAND Panel,"'^ICE'"` Ends a call.
^ICM Modifies an intercom call.	For backwards compatibility, both ^ICM-TALK and ^ICM-LISTEN are supported. In this release, however, the TALK and LISTEN subcommands are ignored. The microphone and/or speaker are activated based on the initial mode value of the intercom start command and the audio data packet flow is started upon receipt of this command by the panel. Syntax: `SEND_COMMAND <DEV>,"`^ICM-TALK`"` Variables: None. Example: `SEND_COMMAND TP1,"`^ICM-TALK`"`
^ICM-MUTEMIC Set the state of the microphone on a panel to muted (1) or unmuted (0).	At the start of each call the microphone starts out unmuted. Syntax: `"'^ICM-MUTEMIC,<state>'"` Variables: 0 - unmuted 1 - muted Example: `SEND_COMMAND Panel, "^ICM-MUTEMIC,1"` Sets the microphone to muted.

Intercom Commands (Cont.)	
^ICS Starts an intercom call to the specified IP address and ports.	Syntax: `^ICS-<IP>,<TX UDP port>,<RX UDP port>,<initial mode>'"` Intercom start. Starts a call to the specified IP address and ports, where initial mode is either 1 (talk) or 0 (listen) or 2 (both). If no mode is specified 0 (listen) is assumed. Please note, however, that no data packets will actually flow until the intercom modify command is sent to the panel. Syntax: `SEND_COMMAND <DEV>,"'^ICS-<IP>,<TX UDP port>,<RX UDP port>,<initial mode>'"` Variables: IP = IP Address of panel to connect with on an Intercom call. TX UDP port = UDP port to transmit to. RX UDP port = UDP port to receive from. initial mode = 0 (listen) or 1 (talk) or 2 (handsfree). 0 is the default. Examples: Example of setting up a handsfree unicast call between two panels: `send_command TP1, "^ICS-192.168.0.3,9000,9002,2"` `send_command TP2, "^ICS-192.168.0.4,9002,9000,2"` Example of setting up a multicast call where the first panel is paging two other panels: `send_command TP1, "^ICS-239.252.1.1,9002,9000,1"` `send_command TP2, "^ICS-239.252.1.1,9002,9000,0"` `send_command TP3, "^ICS-239.252.1.1,9002,9000,0"` Example of setting up a baby monitor call where the first panel is listening to the microphone audio coming from the second panel: `send_command TP1, "^ICS-192.168.0.3,9000,9002,0"` `send_command TP2, "^ICS-192.168.0.4,9002,9000,1"`
^MODEL? Gets the panel model name.	Syntax: `"'^MODEL?'"` Example: `SEND_COMMAND Panel,"'^MODEL?'"` The panel (an MVP-8400i) responds with, ^MODEL-MVP-8400i

SIP Commands

The following table lists and describes SIP commands that are generated from the touch panel.

SIP Commands	
^PHN-AUTOANSWER Provides the state of the auto-answer feature.	Syntax: `"'^PHN-AUTOANSWER, <state>'"` Variable: state = 0 or 1 (off or on) Example: `SEND_COMMAND Panel,"'^PHN-AUTOANSWER, 1'"`
^PHN-CALL Provides call progress notification for a call.	Syntax: `"'^PHN-CALL, <status>, <connection id>'"` Variable: status = CONNECTED, DISCONNECTED, TRYING, RINGING, or HOLD. connection id = The identifying number of the connection. Example: `SEND_COMMAND Panel"'^PHN-CALL, CONNECTED, 1'"` Notifies that the call is connected.

SIP Commands (Cont.)	
^PHN-INCOMING Provides incoming call notification.	Provides incoming call notification and the connection id used for all future commands related to this call. The connection id will be 0 or 1. Syntax: `"'^PHN-INCOMING, <caller number>, <caller name>, <connection id>, <timestamp>, '"` Variable: caller number = The phone number of the incoming call. caller name = The name associated with the caller number. connection id = The identifying number of the connection. timestamp = The current time in MM/DD/YY HH:MM:SS format. Example: `SEND_COMMAND Panel,"'^PHN-INCOMING, 2125551000, AMX, 07/22/08 12:00:00, 1'"`
^PHN-LINESTATE Indicates the current state of each of the available connections used to manage calls.	Syntax: `"'^PHN-LINESTATE, <connection id>, <state>, <connection id>, <state>,...'"` Variable: connection id = The identifying number of the connection. state = IDLE, HOLD, or CONNECTED extn = The local extension of this panel (see Example) Example: `SEND_COMMAND Panel,"'^PHN-LINESTATE, 1, IDLE, 2, CONNECTED, SIP, <extn>'"`
^PHN-MSGWAITING Indicates the number of messages waiting the user's voice mail box.	Syntax: `"'^PHN-MSGWAITING, <messages>, <new message count>, <old message count>, <new urgent message count>, <old urgent message count>'"` Variable: messages = 0 or 1 (1 indicates new messages) new message count = The number of new messages. old message count = The number of old messages. new urgent message count = The number of new messages marked urgent. old urgent message count = The number of old messages marked urgent. Example: `SEND_COMMAND Panel,"'^PHN-MSGWAITING, 1, 1, 2, 1, 0'"`
^PHN-PRIVACY Indicates the state of the privacy feature.	Syntax: `"'^PHN-PRIVACY, <state>'"` Variable: state = 0 (Disable) or 1 (Enable) new message count = The number of new messages. old message count = The number of old messages. new urgent message count = The number of new messages marked urgent. old urgent message count = The number of old messages marked urgent. Example: `SEND_COMMAND Panel,"'^PHN-PRIVACY, 0'"`
^PHN-REDIAL Indicates the panel is redialing the number.	Syntax: `"'^PHN-REDIAL, <number>'"` Variable: number = The phone number to dial. Example: `SEND_COMMAND Panel,"'^PHN-REDIAL, 2125551000'"`

SIP Commands (Cont.)	
^PHN-TRANSFERRED Indicates a call has been transferred.	Syntax: "'^PHN-TRANSFERRED'" Example: SEND_COMMAND Panel,"'^PHN-TRANSFERRED’"

The following table lists and describes SIP commands that are sent to the touch panel to manage calls.

SIP Commands	
^PHN-ANSWER Answers the call.	Syntax: "'^PHN-ANSWER, <connection id>'" Variable: connection id = The identifying number of the connection Example: SEND_COMMAND Panel,"'^PHN-ANSWER, 1'"
^PHN-AUTOANSWER Enables or disables the auto-answer feature of the phone.	Enables (1) or disables (0) the auto-answer feature on the phone. Syntax: "’^PHN-AUTOANSWER, <state>’" Variable: state = 0 (Disable) or 1 (Enable) Example: SEND_COMMAND Panel,"'^PHN-AUTOANSWER, 1'" Enables the auto-answer feature.
?PHN-AUTOANSWER Queries the state of the auto-answer feature.	The panel responds with the ^PHN-AUTOANSWER, <state> message. Syntax: "’?PHN-AUTOANSWER’" Example: SEND_COMMAND Panel,"'?PHN-AUTOANSWER'"
^PHN-CALL Calls the provided number.	Syntax: "’^PHN-CALL, <number>’" Variable: number = The provided phone number Example: SEND_COMMAND Panel,"'^PHN-CALL, 2125551000'"
^PHN-DECLINE Declines the incoming call.	Decline (send to voice mail if configured) the incoming call on <CallID> as indicated from the previous PHN-INCOMING message. CallID should be 0 or 1. Syntax: "'^PHN-DECLINE, <CallID>'" Variable: CallID = The identifying number of the connection. Example: SEND_COMMAND Panel,"'^PHN-DECLINE,0""
^PHN-DTMF Sends DTMF codes.	Syntax: "’^PHN-DTMF, <DTMF code>’" Variable: DTMF code = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, POUND, or ASTERISK. Example: SEND_COMMAND Panel,"'^PHN-DTMF, 1234567879ASTERISK'"

SIP Commands (Cont.)	
^PHN-HANGUP Hangs up the call.	Syntax: "'^PHN-HANGUP, <connection id>'" Variable: connection id = The identifying number of the connection Example: SEND_COMMAND Panel,"'^PHN-HANGUP, 1'"
^PHN-HOLD Places the call on hold.	Syntax: "'^PHN-HOLD, <connection id>'" Variable: connection id = The identifying number of the connection Example: SEND_COMMAND Panel,"'^PHN-HOLD, 1'"
?PHN-LINESTATE Queries the state of each of the connections used by the SIP device.	The panel responds with the ^PHN-LINESTATE message. Syntax: "'?PHN-LINESTATE'" Example: SEND_COMMAND Panel,"'?PHN-LINESTATE'"
^PHN-PRIVACY Enables or disables the privacy feature of the phone.	Enables or disables the privacy feature on the phone (do not disturb). Syntax: "'^PHN-PRIVACY, <state>'" Variable: state = 0 (Disable) or 1 (Enable) Example: SEND_COMMAND Panel,"'^PHN-PRIVACY, 1'" Enables the privacy feature.
?PHN-PRIVACY Queries the state of the privacy feature.	The panel responds with the ^PHN-PRIVACY, <state> message. Syntax: "'?PHN-PRIVACY'" Example: SEND_COMMAND Panel,"'?PHN-PRIVACY'"
^PHN-REDIAL Redials the last number.	Syntax: "'^PHN-REDIAL'" Example: SEND_COMMAND Panel,"'^PHN-REDIAL'"
^PHN-TRANSFER Transfers the call to the provided number.	Syntax: "'^PHN-TRANSFER, <connection id>, <number>'" Variable: connection id = The identifying number of the connection number = The number to which you want to transfer the call. Example: SEND_COMMAND Panel,"'^PHN-TRANSFER, 1, 2125551000'"

The following table lists and describes SIP setup commands. Using any of these commands causes the current user to go offline.

SIP Setup Commands	
^PHN-SETUP-DOMAIN Sets the realm for authentication.	Syntax: "'^PHN-SETUP-DOMAIN,<domain>'" Variable: domain = The realm used for authentication Example: SEND_COMMAND Panel,"'^PHN-SETUP-DOMAIN,asterisk'"
^PHN-SETUP-ENABLE Registers a new user	Once the configuration has been updated, the ENABLE command should be run to re-register the new user. Syntax: "'^PHN-SETUP-ENABLE'"
^PHN-SETUP-PASSWORD Sets the user password for the proxy server.	Syntax: "'^PHN-SETUP-PASSWORD,<password>'" Variable: password = The password for the user name Example: SEND_COMMAND Panel,"'^PHN-SETUP-PASSWORD,6003'"
^PHN-SETUP-PORT Sets the port number for the proxy server.	Syntax: "'^PHN-SETUP-PORT,<port>'" Variable: port = The port for the proxy server Example: SEND_COMMAND Panel,"'^PHN-SETUP-PORT,5060'"
^PHN-SETUP-PROXYADDR Sets the IP address for the proxy server.	Syntax: "'^PHN-SETUP-PROXYADDR,<IP>'" Variable: IP = The IP address for the proxy server Example: SEND_COMMAND Panel,"'^PHN-SETUP-PROXYADDR,192.168.223.111'"
^PHN-SETUP-STUNADDR Sets the IP address for the STUN server.	Syntax: "'^PHN-SETUP-STUNADDR,<IP>'" Variable: IP = The IP address for the STUN server Example: SEND_COMMAND Panel,"'^PHN-SETUP-STUNADDR,192.168.223.111'"
^PHN-SETUP-USERNAME Sets the user name for authentication with the proxy server.	Syntax: "'^PHN-SETUP-USERNAME,<username>'" Variable: username = The user name (usually the phone extension) Example: SEND_COMMAND Panel,"'^PHN-SETUP-USERNAME,6003'"

Appendix A: Text Formatting

Text Formatting Codes for Bargraphs/Joysticks

Text formatting codes for bargraphs provide a mechanism to allow a portion of a bargraphs text to be dynamically provided information about the current status of the level (multistate and traditional). These codes are entered into the text field along with any other text.

The following is a code list used for bargraphs:

Bargraph Text Code Inputs		
Code	**Bargraph**	**Multi-State Bargraph**
$P	Display the current percentage of the bargraph (derived from the Adjusted Level Value as it falls between the Range Values)	Display the current percentage of the bargraph (derived from the Adjusted Level Value as it falls between the Range Values)
$V	Raw Level Value	Raw Level Value
$L	Range Low Value	Range Low Value
$H	Range High Value	Range High Value
$S	N/A	Current State
$A	Adjusted Level Value (Range Low Value subtracted from the Raw Level Value)	Adjusted Level Value (Range Low Value subtracted from the Raw Level Value)
$R	Low Range subtracted from the High Range	Low Range subtracted from the High Range
$$	Dollar sign	Dollar sign

Buy changing the text on a button (via a VT command) you can modify the codes on a button. When one of the Text Formatting Codes is encountered by the firmware it is replaced with the correct value. These values are derived from the following operations:

Formatting Code Operations	
Code	**Operation**
$P	(Current Value - Range Low Value / Range High Value - Range Low Value) x 100
$V	Current Level Value
$L	Range Low Value
$H	Range High Value
$S	Current State (if regular bargraph then resolves to nothing)
$A	Current Value - Range Low Value
$R	Range High Value - Range Low Value

Given a current raw level value of 532, a range low value of 500 and a high range value of 600 the following text formatting codes would yield the following strings as shown in the table below:

Example	
Format	**Display**
$P%	32%
$A out of $R	32 out of 100
$A of 0 - $R	32 of 0 - 100
$V of $L - $H	532 of 500 - 600

Text Area Input Masking

Text Area Input Masking can be used to limit the allowed/correct characters that are entered into a text area. For example, in working with a zip code, a user could limit the entry to a max length of only 5 characters but, with input masking, you could limit them to 5 mandatory numerical digits and 4 optional numerical digits. A possible use for this feature is to enter information into form fields. The purpose of this feature is to:

- Force you to use correct type of characters (i.e. numbers vs. characters)
- Limit the number of characters in a text area
- Suggest proper format with fixed characters
- Right to Left
- Required or Optional
- Change/Force a Case
- Create multiple logical fields
- Specify range of characters/number for each field

With this feature, it is NOT necessary to:

- Limit you to a choice of selections
- Handle complex input tasks such as names, days of the week or month by name
- Perform complex validation such as Subnet Mask validation

Input mask character types

These character types define what information is allowed to be entered in any specific instance. The following table lists what characters in an input mask will define what characters are allowed in any given position.

Character Types	
Character	**Masking Rule**
0	Digit (0 to 9, entry required, plus [+] and minus [-] signs not allowed)
9	Digit or space (entry not required, plus and minus signs not allowed)
#	Digit or space (entry not required; plus and minus signs allowed)
L	Letter (A to Z, entry required)
?	Letter (A to Z, entry optional)
A	Letter or digit (entry required)
a	Letter or digit (entry optional)
&	Any character or a space (entry required)
C	Any character or a space (entry optional)

The number of the above characters used determines the length of the input masking box. Example: 0000 requires an entry, requires digits to be used, and allows only 4 characters to be entered/used.

Refer to the following Send Commands for more detailed information:

- ^BIM - Sets the input mask for the specified addresses. (see the *^BIM* section on page 149).
- ^BMF subcommand **%MK** - sets the input mask of a text area (see the *^BMF* section on page 150).

Input mask ranges

These ranges allow a user to specify the minimum and maximum numeric value for a field. ***Only one range is allowed per field. Using a range implies a numeric entry ONLY.***

Input Mask Ranges	
Character	**Meaning**
[	Start range
]	End range
|	Range Separator

An example from the above table:

[0|255] This allows a user to enter a value from 0 to 255.

Input mask next field characters

These characters allow you to specify a list of characters that cause the keyboard to move the focus to the next field when pressed instead of inserting the text into the text area.

Input Mask Next Field Char	
Character	**Meaning**
{	Start Next Field List
}	End Next Field List

An example from the above table:

{.} or {:} or {.:} Tells the system that after a user hits any of these keys, proceed to the next text area input box.

Input mask operations

Input Mask Operators change the behavior of the field in the following way:

Input Mask Operators	
Character	**Meaning**
<	Forces all characters to be converted to lowercase
>	Forces all characters to be converted to uppercase
^	Sets the overflow flag for this field

Input mask literals

To define a literal character, enter any character, other than those shown in the above table *(including spaces, and symbols)*. A back-slash ('\') causes the character that follows it to be displayed as the literal character. For example, **\A** is displayed just as the letter **A**. To define one of the following characters as a literal character, precede that character with a back-slash. Text entry operation using Input Masks.

A keyboard entry using normal text entry is straightforward. However, once an input mask is applied, the behavior of the keyboard needs to change to accommodate the input mask's requirement. When working with masks, any literal characters in the mask will be "skipped" by any cursor movement including cursor keys, backspace, and delete.

When operating with a mask, the mask should be displayed with placeholders. The "-" character should display where you should enter a character. The arrow keys will move between the "-" characters and allow you to replace them. The text entry code operates as if it is in the overwrite mode. If the cursor is positioned on a character already entered and you type in a new (and valid) character, the new character replaces the old character. There is no shifting of characters.

When working with ranges specified by the [] mask, the keyboard allows you to enter a number between the values listed in the ranges. If a user enters a value that is larger than the max, the maximum number of right-most characters is used to create a new, acceptable value.

- **Example 1**: If you type "125" into a field accepting 0-100, then the values displayed will be "1", "12", "25".
- **Example 2**: If the max for the field was 20, then the values displayed will be "1", "12", "5".

When data overflows from a numerical field, the overflow value is added to the previous field on the chain, **if** the overflow character was specified. In the above example, if the overflow flag was set, the first example will place the "1" into the previous logical field and the second example will place "12" in the previous logical field. If the overflow field already contains a value, the new value will be inserted to the right of the current characters and the overflow field will be evaluated. Overflow continues to work until a field with no overflow value is set or there are no more fields left (i.e. reached first field).

If a character is typed and that character appears in the Next Field list, the keyboard should move the focus to the next field. For example, when entering time, a **":"** is used as a next field character. If you hit "1:2", the 1 is entered in the current field (hours) and then the focus is moved to the next field and 2 is entered in that field.

When entering time in a 12-hour format, entry of AM and PM is required. Instead of adding AM/PM to the input mask specification, the AM/PM should be handled within the NetLinx code. This allows a programmer to show/hide and provide discrete feedback for AM and PM.

Input mask output examples

The following are some common input masking examples:

Output Examples		
Common Name	**Input Mask**	**Input**
IP Address Quad	[0|255]{.}	Any value from 0 to 255
Hour	[1|12]{:}	Any value from 1 to 12
Minute/Second	[0|59]{:}	Any value from 0 to 59
Frames	[0|29]{:}	Any value from 0 to 29
Phone Numbers	(999) 000-0000	(555) 555-5555
Zip Code	00000-9999	75082-4567

URL Resources

A URL can be broken into several parts. For example: the URL *http://www.amx.com/company-info-home.asp*. This URL indicates that the protocol in use is **http** (HyperText Transport Protocol) and that the information resides on a host machine named **www.amx.com**. The image on that host machine is given an assignment (*by the program*) name of **company-info-home.asp** *(Active Server Page)*.

The exact meaning of this name on the host machine is both protocol dependent and host dependent. The information normally resides in a file, but it could be generated dynamically. This component of the URL is called the file component, even though the information is not necessarily in a file.

A URL can optionally specify a port, which is the port number to which the TCP/IP connection is made on the remote host machine. If the port is not specified, the default port for the protocol is used instead. For example, the default port for http is 80. An alternative port could be specified as: http://www.amx.com:8080/company-info-home.asp.

You can use any legal HTTP syntax.

Special escape sequences

The system has only a limited knowledge of URL formats in that it transparently passes the URL information onto the server for translation. A user can then pass any parameters to the server side programs such as CGI scripts or active server pages. However; the system will parse the URL looking for special escape codes. When it finds an escape code it replaces that code with a particular piece of panel, button, or state information. For example, "http://www.amx.com/img.asp?device=$DV" would become "http://www.amx.com/img.asp?device=10001". Other used escape sequences include:

Escape Sequences	
Sequence	**Panel Information**
$DV	Device Number
$SY	System Number
$IP	IP Address
$HN	Host Name
$MC	Mac Address
$ID	Neuron ID
$PX	X Resolution of current panel mode/file
$PY	Y Resolution of current panel mode/file
$BX	X Resolution of current button
$BY	Y Resolution of current button
$BN	Name of button
$ST	Current state
$AC	Address Code
$AP	Address Port
$CC	Channel Code
$CP	Channel Port
$LC	Level Code
$LP	Level Port

Appendix B - Wireless Technology

Overview of Wireless Technology

- **802.11b/2.4 GHz and 802.11a/5 GHz** are the two major WLAN standards and both operate using radio frequency (RF) technology. Together the two standards are together called Wi-Fi and operate in frequency bands of 2.4 GHz and 5 GHz respectively.
  The ***802.11b*** specification was the first to be finalized and reach the marketplace. The actual throughput you can expect to obtain from an 802.11b network will typically be between 4 and 5 Mbps.
  Because of the higher frequency (and thus shorter wavelength) that they use, ***802.11a*** signals have a much tougher time penetrating solid objects like walls, floors, and ceilings. As a result, the price for 802.11a's higher speed is not only shorter in range but also a weaker and less consistent signal.
  802.11g provides increased bandwidth at 54 Mbps. As part of the IEEE 802.11g specification, when throughput cannot be maintained, this card will automatically switch algorithms in order to maintain the highest spread possible at a given distance. In addition, 802.11g can also step down to utilize 802.11b algorithms and also maintain a connection at longer distances.
- IP Routing is a behavior of the wireless routing is largely dependent on the wired network interface. Although the panel can be connected to two networks simultaneously it may only have one gateway. If the wired network was successfully set up and a gateway was obtained; then the default route for all network traffic will be via the wired network. In the event that the wired network was not configured, then the default route for all network traffic will be via the wireless network. The wired network connection always takes priority.
  - As an example: Imagine a panel connected to two networks A & B. A is the wired network and B is the wireless network. If the Master controller is on either of these networks then it will be reached. However if the Master controller is on a different network, C, then determining which network interface (wired or wireless) that will be used is dependent on the gateway.
- **Wireless Access Points** are the cornerstone of any wireless network. A Wireless Access Point acts as a bridge between a wired and wireless network. It aggregates the traffic from all the wireless clients and forwards it down the network to the switch or router.
  One Wireless Access Point may be all you need. However, you could need more Wireless Access Points depending on either how large your installation is, how it is laid out, and how it is constructed.
- **Wireless Equivalent Privacy** (**WEP**) Security is a method by which WLANs protect wireless data streams. A data stream encrypted with WEP can still be intercepted or eavesdropped upon, but the encryption makes the data unintelligible to the interloper. The strength of WEP is measured by the length of the key used to encrypt the data. The longer the key, the harder it is to crack.
  802.11b implementations provided 64-bit and 128-bit WEP keys. This is known respectively as 64-bit and 128-bit WEP encryption. 64-bit is generally not regarded as adequate security protection. Both key lengths are supported by the Modero product line.
  Whichever level of WEP you use, it's ***crucial to use identical settings (CASE SENSITIVE)***--the key length, and the key itself-- on all devices. Only devices with common WEP settings will be able to communicate. Similarly, if one device has WEP enabled and another doesn't, they won't be able to talk to each other.

  Although the calculations required to encrypt data with WEP can impact the performance of your wireless network, it's generally seen only when running benchmarks, and not large enough to be noticeable in the course of normal network usage.

Terminology

- **802.1x**
  - IEEE 802.1x is an IEEE standard that is built on the Internet standard EAP (Extensible Authentication Protocol). 802.1x is a standard for passing EAP messages over either a wired or wireless LAN. Additionally, 802.1x is also responsible for communicating the method with which WAPs and wireless users can share and change encryption keys. This continuous key change helps resolve any major security vulnerabilities native to WEP.
- **AES**
  - Short for Advanced Encryption Standard, is a cipher currently approved by the NSA to protect US Government documents classified as Top Secret. The AES cipher is the first cipher protecting Top Secret information available to the general public.
- **CERTIFICATES (CA)**
  - A certificate can have many forms, but at the most basic level, a certificate is an identity combined with a public key, and then signed by a certification authority. The certificate authority (CA) is a trusted external third party which "signs" or validates the certificate. When a certificate has been signed, it gains some cryptographic properties. AMX supports the following security certificates within three different formats:
    - **PEM** (Privacy Enhanced Mail)
    - **DER** (Distinguished Encoding Rules)
    - **PKCS12** (Public Key Cryptography Standard #12)
  - Typical certificate information can include the following items:
    - Certificate Issue Date
    - Extensions
    - Issuer
    - Public Key
    - Serial Number
    - Signature Algorithm
    - User
    - Version
- **MIC**
  - Short for Message Integrity Check, prevents forged packets from being sent. Through WEP it was possible to alter a packet whose content was known even if it had not been decrypted.
- **TKIP**
  - Short for Temporal Key Integration, is part of the IEEE 802.11i encryption standard for wireless LANs. TKIP provides per-packet key mixing, message integrity check and re-keying mechanism, thus ensuring every data packet is sent with its own unique encryption key. Key mixing increases the complexity of decoding the keys by giving the hacker much less data that has been encrypted using any one key.
- **WEP**
  - Short for Wired Equivalent Privacy (WEP), is a scheme used to secure wireless networks (Wi-Fi). A wireless network broadcasts messages using radio which are particularly susceptible to hacker attacks. WEP was intended to provide the confidentiality and security comparable to that of a traditional wired network. As a result of identified weaknesses in this scheme, WEP was superseded by Wi-Fi Protected Access (WPA), and then by the full IEEE 802.11i standard (also known as WPA2).

- **WPA**
  - Wi-Fi Protected Access (WPA and WPA2) is a class of system used to secure wireless (Wi-Fi) computer networks. It was created in response to several serious weaknesses researchers had found in the previous WEP system. WPA implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared (WPA2).
  - WPA is designed to work with all wireless network interface cards, but not necessarily with first generation wireless access points.
  - To resolve problems with WEP, the Wi-Fi Alliance released WPA (FIG. 98) which integrated **802.1x**, **TKIP** and **MIC**. Within the WPA specifications the RC4 cipher engine was maintained from WEP. RC4 is widely used in SSL (Secure Socket Layer) to protect internet traffic.

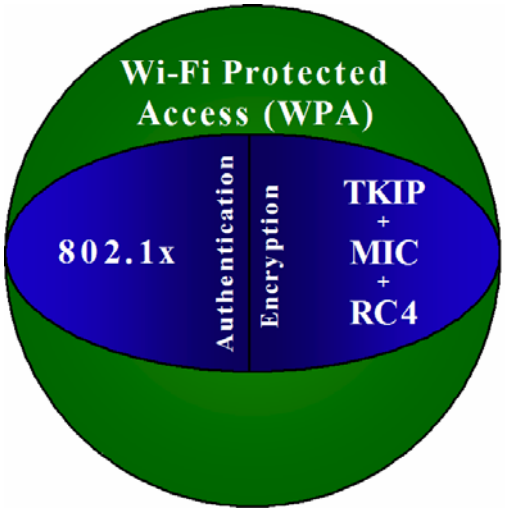


FIG. 98 WPA Overview

- **WPA2**
  - Also know as IEEE 802.11i, is an amendment to the 802.11 standard specifying security mechanisms for wireless networks. The 802.11i scheme makes use of the Advanced Encryption Standard (AES) block cipher; WEP and WPA use the RC4 stream cipher.
  - The 802.11i architecture contains the following components: 802.1X for authentication (entailing the use of EAP and an authentication server), RSN for keeping track of associations, and AES-based CCMP to provide confidentiality, integrity and origin authentication.
  - WPA2 implements the full standard, but will not work with some older network cards. Both provide good security, with two significant issues:
    - *either WPA or WPA2 must be enabled and chosen in preference to WEP. WEP is usually presented as the first security choice in most installation instructions.*
    - *in the "Personal" mode, the most likely choice for homes and small offices, a passphrase is required that, for full security, must be longer than the typical 6 to 8 character passwords users are taught to employ.*
  - With the RC4 released to the general public the IEEE implemented the Advanced Encryption Standard (AES) as the cipher engine for 802.11i, which the Wi-Fi Alliance has branded as WPA2.

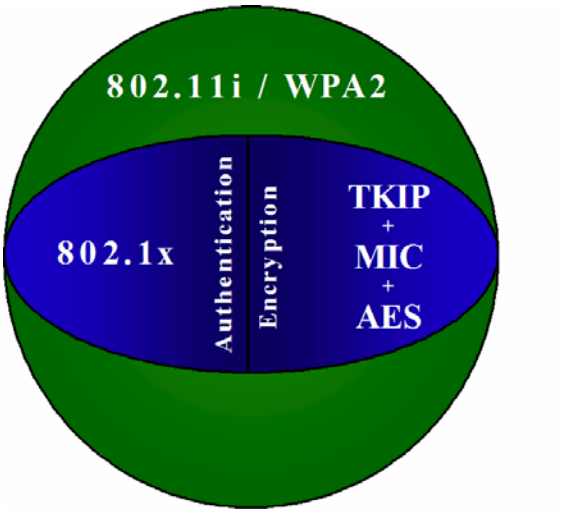


FIG. 99 WPA2 Overview

EAP Authentication

EAP (Extensible Authentication Protocol) is an Enterprise authentication protocol that can be used in both a wired and wireless network environment. EAP requires the use of an 802.1x Authentication Server, also known as a Radius server. Although there are currently over 40 different EAP methods defined, the current internal Modero 802.11g wireless card and accompanying firmware only support the following EAP methods (***listed from simplest to most complex***):

- EAP-LEAP (Cisco Light EAP)
- EAP-FAST (Cisco Flexible Authentication via Secure Tunneling, a.k.a. LEAPv2)

The following use certificates:

- EAP-PEAP (Protected EAP)
- EAP-TTLS (Tunneled Transport Layer Security)
- **EAP-TLS** (Transport Layer Security)

EAP requires the use of an 802.1x authentication server (also known as a Radius server). Sophisticated Access Points (such as Cisco) can use a built-in Radius server. The most common RADIUS servers used in wireless networks today are:

- Microsoft Sever 2003
- Juniper Odyssey (once called Funk Odyssey)
- Meetinghouse AEGIS Server
- DeviceScape RADIUS Server
- Cisco Secure ACS

EAP characteristics

The following table outlines the differences among the various EAP Methods from most secure (at the top) to the least secure (at the bottom of the list):

EAP Method Characteristics

Method:	Credential Type:	Authentication:	Pros:	Cons:
EAP-TLS	• Certificates	• Certificate is based on a two-way authentication	• Highest Security	• Difficult to deploy
EAP-TTLS	• Certificates • Fixed Passwords • One-time passwords (tokens)	• Client authentication is done via password and certificates • Server authentication is done via certificates	• High Security	• Moderately difficult to deploy
EAP-PEAP	• Certificates • Fixed Passwords • One-time passwords (tokens)	• Client authentication is done via password and certificates • Server authentication is done via certificates	• High Security	• Moderately difficult to deploy
EAP-LEAP	• Certificates • Fixed Passwords • One-time passwords (tokens)	• Authentication is based on MS-CHAP and MS-CHAPv2 authentication protocols	• Easy deployment	• Susceptible to dictionary attacks
EAP-FAST	• Certificates • Fixed Passwords • One-time passwords (tokens)	• N/A	• N/A	• N/A

EAP communication overview

EAP Authentication goes a step beyond just encrypting data transfers, but also requires that a set of credentials be validated before the client (panel) is allowed to connect to the rest of the network (FIG. 100). Below is a description of this process. It is important to note that there is no user intervention necessary during this process. It proceeds automatically based on the configuration parameters entered into the panel.

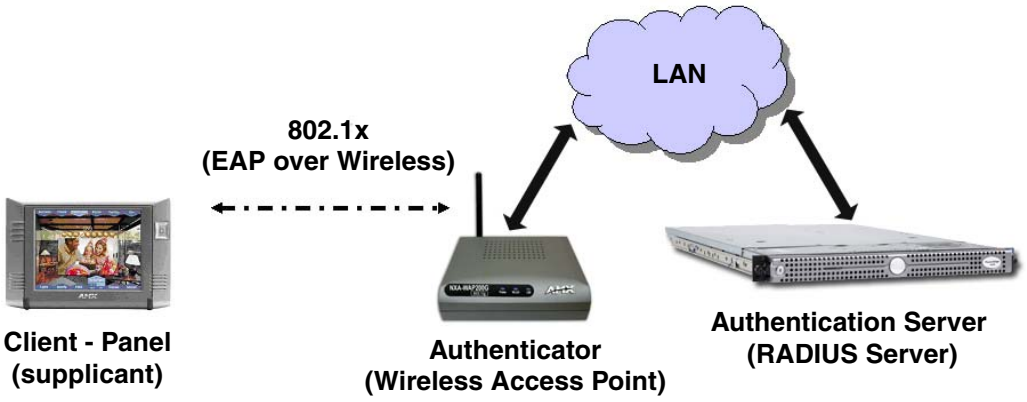


FIG. 100 EAP security method in process

1. The client (panel) establishes a wireless connection with the WAP specified by the SSID.
2. The WAP opens up a tunnel between itself and the RADIUS server configured via the access point. This tunnel means that packets can flow between the panel and the RADIUS server but nowhere else. ***The network is protected until authentication of the client (panel) is complete and the ID of the client is verified.***
3. The WAP (Authenticator) sends an "EAP-Request/Identity" message to the panel as soon as the wireless connection becomes active.
4. The panel then sends a "EAP-Response/Identity" message through the WAP to the RADIUS server providing its identity and specifying which EAP type it wants to use. If the server does not support the EAP type, then it sends a failure message back to the WAP which will then disconnect the panel. As an example, EAP-FAST is only supported by the Cisco server.
5. If the EAP type is supported, the server then sends a message back to the client (panel) indicating what information it needs. This can be as simple as a username (*Identity*) and password or as complex as multiple CA certificates.
6. The panel then responds with the requested information. If everything matches, and the panel provides the proper credentials, the RADIUS server then sends a success message to the access point instructing it to allow the panel to communicate with other devices on the network. At this point, the WAP completes the process for allowing LAN Access to the panel (possibly a restricted access based on attributes that came back from the RADIUS server).
    - As an example, the WAP might switch the panel to a particular VLAN or install a set of firewall rules.

AMX Certificate Upload Utility

The Certificate Upload utility gives you the ability to compile a list of target touch panels, select a pre-obtained certificate (uniquely identifying the panel), and then upload that file to the selected panel.

NOTE

This application must be run from a local machine and should not be used from a remote network location.

This application ensures that a unique certificate is securely uploaded to a specific touch panel. Currently, the target panels must be capable of supporting the WPA-PSK and EAP-XXX wireless security formats.

The Certificate Upload utility supports the following capabilities:

- Ability to browse both a local and network drive to find a desired certificate file.
- Ability to create a list of target AMX G4 touch panels based on IP Addresses
  - Compatible panels include: MVP-8400, MVP-7500, NXD-CV10, NXT-CV10, NXD-CV7, NXT-CV7, NXD-700Vi, and NXD-1000Vi.
- Ability to display the IP Address of the local computer hosting the application.
- Ability to load a previously created list of target touch panels.
- Ability to save the current list of target Modero panel as a file.
- Ability to track the progress of the certificate upload by noting the current data size being transmitted and any associated error messages (if any).

The Certificate Upload Utility recognizes the following certificate file types:

- **CER** (Certificate File)
- **DER** (Distinguished Encoding Rules)
- **PEM** (Privacy Enhanced Mail)
- **PFX** (Normal Windows generated certificate)
- **PVK** (Private Key file)

Configuring your G4 Touch Panel for USB Communication

For a personal computer to establish a connection to a Modero panel via USB, the target computer must have the appropriate AMX USB driver installed. This installation is bundled into the latest TPDesign4 and NetLinx Studio2 software setup process or can be downloaded independently from the main Application Files page on www.amx.com.

NOTE

Close the Certificate Upload Utility before configuring the touch panel's USB driver. Only after the panel has been successfully setup to communicate via USB can you then re-launch the utility.

Step 1: Setup the Panel and PC for USB Communication

1. If you do not currently have the latest version of TPDesign4, navigate to **www.amx.com > Tech Center > Downloadable Files > Application Files > NetLinx Design Tools** section of the website and locate the AMX USB Driver executable (AMX USBLAN Setup exe).
2. Download this executable file to a known location on your computer.
3. Launch the Setup.exe and follow the on-screen prompts to complete the installation.

Step 2: Confirm the Installation of the USB Driver on the PC

The first time each AMX touch panel is connected to the PC it is detected as a new hardware device and the USBLAN driver becomes associated with it (panel specific). Each time thereafter the panel is "recognized" as a unique USBLAN device and the association to the driver is done in the background. When the panel is detected for the first time some user intervention is required during the association between panel and driver.

1. After the installation of the USB driver has been completed, confirm the proper installation of the large Type-A USB connector to the PC's USB port, and restart your machine.

If the panel is already powered, continue with steps 3. The panel MUST be powered and configured for USB communication before connecting the mini-USB connector to the panel's Program Port.

2. Connect the terminal end of the power cable to the 12 VDC power connector on the side/rear of the pane, and supply power. If using an MVP that is installed onto a docking station, feed power to the docked panel by connecting the appropriate power supply to the docking station.
   After the panel powers-up, access the firmware setup pages by either:
   - **MVP** - Pressing and holding the two lower buttons on both sides of the display for 3 seconds.
   - **CV7/CV10** - Pressing the grey Front Setup Access button for 3 seconds.
   - **700Vi/1000Vi** - Pressing the grey Front Setup Access button for 3 seconds.
3. Select Protected Setup > System Settings (located on the lower-left) to open the System Settings page.
4. Toggle the blue *Type* field (from the Master Connection section) until the choice cycles to **USB**.
   - The connection remains RED after changing the communication from Ethernet to USB until the panel is rebooted.
   - Once the panel restarts, the connection turns a dark green until connected to an active USB cable.
5. Press the **Back** button on the touch panel to return to the Protected Setup page.
6. Press the on-screen **Reboot** button to both save any changes and restart the panel. Remember that the panel's connection type must be set to USB prior to rebooting the panel and prior to inserting the USB connector.
7. **ONLY AFTER** the unit displays the first panel page, **THEN** insert the mini-USB connector into the Program Port on the panel.
   - It may take a minute for the panel to detect the new connection and send a signal to the PC (indicated by a green System Connection icon). If this is your first time installing the USB driver, a USB driver installation popup window appears on the PC.
8. Complete the USB driver installation process by clicking **Yes** and then installing the new AMX USB LAN LINK when told that a new USB device was found. This action accepts the installation of the new AMX USB driver.
9. Reboot the panel. Once restarted, the panel is now configured to communicate directly with the PC.

The mini-USB connector MUST be then plugged into an already active panel before the PC can recognize the connection and assign an appropriate USB driver. This driver is part of both the NetLinx Studio and TPDesign4 software application installations.

10. Launch the Certificate Upload Utility and confirm the utility has detected the new USB connection to the panel:
    - Click on the ***Local Address*** field's drop-down arrow.
    - Confirm the new USB entry shows up in the list as: **10.XX.XX.1**.

How to Upload a Certificate File

1. Install the latest AMX USB LAN LINK driver onto your computer by installing the latest versions of either TPDesign4 or NetLinx Studio2. This USB driver prepares your computer to properly communicate with a directly connected G4 touch panel (MVP/CV7/CV10/700Vi/1000Vi).
   - Refer to Step 1 from within the previous *Step 1: Setup the Panel and PC for USB Communication* section on page 203.
2. Access the target panel's Protected Setup firmware page and configure the USB communication parameters.
   - Refer to Step 2 from within the previous *Step 2: Confirm the Installation of the USB Driver on the PC* section on page 204.
3. With the panel successfully communicating with target computer, launch the Certificate Upload Utility.
   - Familiarize yourself with the User Interface options (Certificate Utility User Interface).
4. Locate your certificate file by using the **Browse** button and navigating to the desired file type.
5. Use the drop-down arrow in the *Local Address* field to select communication through either the computer's Ethernet port (Internet communication) or via the USB port (direct connection). If using an Ethernet connection skip to step 8.
6. **For a USB connection**, select the ***10.XX.XX.1*** IP Address which corresponds to the virtual IP Address assigned to the USB connection port on the computer.
7. **For a USB connection**, navigate to the *Add IP Address* field (bottom-right of the interface) and enter a value of **1** greater than the virtual USB IP Address.
   - For example: If the virtual USB IP Address is **10.0.0.1** then you would add an address for the directly connected panel of **10.0.0.2** (this is one greater than the USB address value detected by the utility).
   - **You can send a certificate to ONLY ONE directly connected panel (via USB)**. If using the Ethernet port's IP Address, you can send a server certificate to multiple target panels.
8. **For an Ethernet IP Address connection**, select the IP Address which corresponds to the local computer's Ethernet address.
9. Navigate to the *Add IP Address* field (bottom-right of the interface) and enter the IP Addresses of the various target touch panels.
10. Click the **Add** button to complete the entry and add the new IP Address to the listing of available device IP Addresses. Repeat this process for all subsequent device IP Addresses.
11. Once your list is complete, click on the **File** drop-down menu and select the **Save** option to launch a Save dialog where you can assign a name to the current list of addresses and then save the information (as a TXT (text) file) to a known location.

This application must be run from a local machine and should not be used from a remote network location.

12. Select the target devices which be uploaded with the selected certificate. These can either be:
    - individually selected by toggling the box next to the Send entry (with the Type column).
    - selected as a group by clicking on the Check All radio box located at the top of the device IP Address listing.
13. When you are ready to send the certificate file to the selected panels, click the **Send** button to initiate the upload.
    - Once the *Status* field for each entry reads **Done**, your upload was successfully completed.

Appendix C: Troubleshooting

This section describes the solutions to possible hardware/firmware issues that could arise during the common operation of a Modero touch panel.

Troubleshooting Information	
Symptom	**Solution**
My USB drivers has a yellow exclamation point and doesn't appear to be working.	The USB driver was incorrectly installed and should be re-installed: • Power up the panel without the USB cable connected to the panel. • Plug in the USB cable into the G4 panel. You should see a USB icon show up in the System Tray. • Double click on the icon to bring up the list of USB devices (you should see the "AMX USB LAN LINK" device in the list). • If the "Install Driver" dialog doesn't appear automatically, select the "Properties" button and then the "Update Driver" button. • When the Install Driver dialog does appear, click Next to accept all the default prompts. • The OS will notify you that the driver you are installing/updating does not have a digital signature. This is acceptable, agree to continue the installation. • After installation is complete, the exclamation point should disappear.
When using G4 WebControl to communicate with a target panel, a VNC Server dialog appears on my screen.	• During a WebControl connection to a target panel you are prompted with a G4 Authentication dialog which asks you to enter the assigned password for the panel (before gaining access). • If you are ever prompted with a VNC Server dialog, you must enter the IP Address of the target panel. This can be found within the **Setup** > **Protected Setup** > System Settings page. - This IP Address of the panel appears within the IP Settings section of this page • Enter the IP Address and click **OK**. You will then be prompted with the G4 Authentication popup where you must enter the panel's WebControl password.
While attempting to communicate directly with the Virtual Master (on the PC) via a USB connection, I can't get my communication icon to turn Green.	• A Green communication icon indicates that a connection has been established to the target Master or target Virtual Master. • Launch NetLinx Studio and configure the Master Connection communication settings for a Virtual Master. • Navigate to the System Settings page and toggle the *Type* field to **USB**. • Make sure the Type-A USB connector is securely connected to the PC. • Make sure the panel DOESN'T have the mini-USB connected and TURN OFF the panel. • Once the panel has turned ON THEN connect the mini-USB to the Program Port. The USB icon should appear in your system tray. If it doesn't. • The panel can take a few minutes to detect the connection to the PC.
My Modero panel isn't appearing in my Workspace window.	• Verify that the System number is the same on both the NetLinx Workspace window and the System Settings page on the Modero panel. • Verify you have entered the proper NetLinx Master IP and connection methods into the Master Connection section of the System Settings page.

Troubleshooting Information (Cont.)	
Symptom	**Solution**
My Modero panel can't obtain a DHCP Address	In requesting a DHCP Address, the DHCP Server can take up to a few minutes to provide the address. • Verify there is an active Ethernet connection attached to the rear of the Modero before beginning these procedures. • Select **Diagnostics** > **Network Address**, from the Main menu and verify the System number. • If the IP Address field is still empty, give the Modero a few minutes to negotiate a DHCP Address and try again.
My panel is not showing up in the Virtual Master's System list of connected devices.	If you a Virtual Master has already connected to the target panel, the G4 device retains the information of the previous Virtual Master System number. • Reboot the panel without the USB cable plugged into the panel. • Configure NetLinx Studio for a Virtual Master connection. Note the System Number used in the Edit Settings window. • Stop communication on the Virtual Master by going to **Settings** > **Stop Communications**. • Click **Yes** to stop communication. • Select the System Number (from the Online Tree tab) and use a right mouse click to select **Refresh System**. This re-establishes communication with the Virtual Master. • Plug-in the mini-USB cable into the corresponding port on the panel. • Wait a few seconds and refresh the system. This re-establishes communication with the Virtual Master. The panel should now appear in the list of available devices.
My Connection Status button isn't blinking and it says the USB is connecting.	"USB Connecting" is displayed when the panel is trying to establish USB communication with the PC (either within the NetLinx Studio or TPDesign4 applications). • Remove the USB connector from the panel and close any AMX applications. • Reboot the panel. • Launch the AMX application and attempt reconnect to the panel. • If using Studio for Virtual Master communication, establish a Virtual Master connection, verify the correct System number, stop communication with the Virtual Master, and then re-establish communication by refreshing the system. • After the panel powers-up, reconnect the USB connector to the panel. • Verify that you have a valid USB connection from within your System Tray.
My on-screen mouse cursor doesn't appear.	• The USB connections are not detected until after the particular USB connection plugged into the corresponding port on the panel and power is cycled to the panel.
Calibration is not working.	• After the Modero touch panel has been updated with a new firmware kit (downloaded to the panel through NetLinx Studio), the calibration could need to be reset. • Cycling power to the panel should provide a baseline calibration for the particular touch panel. Proceed to the Calibration page and reset the on-screen calibration.
Panel doesn't respond to my touches	• The protective cover acts to press on the entire LCD and makes calibration difficult because the user can't calibrate on specific crosshairs when the sheet is pressing on the whole LCD. • Verify that the protective laminate coating on the LCD is removed before beginning any calibration process.

Troubleshooting Information (Cont.)	
Symptom	**Solution**
There is a crawling, dashed line on the left border of the graphics.	• On some units at some resolutions, there are wavy lines across the entire screen. This has been seen on middle resolutions and is referred to as the "Mid Range Fallout" problem. • This is due to the graphics controller settings in the firmware. • Update to the latest v2.XX.XX firmware. • Visit the **www.amx.com** > T**ech Center** > **Downloadable Files** > **Firmware Files** > **Modero panels**. Then Download the KIT file to your computer.
My WEP doesn't seem to be working.	• WEP will not work unless the same default key is set on both the panel and the Access Point. • For example: if you had your access point set to default key 4 (which was 01:02:03:04:05) you must also set the Modero's panel key 4 to 01:02:03:04:05.
NetLinx Studio only detects one of my connected Masters.	Each Master is give a Device Address of 00000. • Only one Master can be assigned to a particular System number. If you want to work with multiple Masters, open different instances of NetLinx Studio and assign each Master its own System value. • Example: a site has an NXC-ME260/64 and an NI-4000. In order to work with both units. The ME260/64 can be assigned System #1 and the NI-4000 can then be assigned System #2 using two open sessions of NetLinx Studio 2.
I can't seem to connect to a NetLinx Master using my NetLinx Studio 2.x application.	• From the **Settings** > **Master Comm Settings** > **Communication Settings** > **Settings (for TCP/IP)**, uncheck the "**Automatically Ping the Master Controller** to ensure availability". • The pinging is to determine if the Master is available, and to reply with a connection failure instantly if it is not. Without using the ping feature, you will still attempt to make a connection, but a failure will take longer to be recognized. Some firewalls and networks do not allow pinging, though, and the ping will then always result in a failure. • When connecting to a NetLinx Master controller via TCP/IP, the program will first try to ping the controller before attempting a connection. Pinging a device is relatively fast and will determine if the device is off-line, or if the TCP/IP address that was entered was incorrect. If you decide NOT to ping for availability and the controller is off-line, or you have an incorrect TCP/IP address, the program will try for 30-45 seconds to establish a connection. ***Note**:* If you are trying to connect to a master controller that is behind a firewall, you may have to uncheck this option. Most firewalls will not allow ping requests to pass through for security reasons.
I have more that one Modero panel connected to my System Master and only one shows up.	Multiple NetLinx Compatible devices (such as Modero panels) can be associated for use with a single Master. Each Modero panel comes with a defaulted Device Number value of 10001. When using multiple panels, it can become very easy to overlook the need to assign different Device Number values to each panel. • Press and hold the grey Front Setup Access button for 3 seconds to open the Setup page. • Press the **Protected Setup** button (located on the lower-left of the panel page), enter ***1988*** into the on-screen Keypad's password field, and press **Done** when finished. • Enter a Device Number value for the panel into the Device Number Keypad. *The default is 10001 and the range is from 1 - 32000*.

Troubleshooting Information (Cont.)	
Symptom	**Solution**
I have more that one Modero panel connected to my System Master and only one shows up.	Multiple NetLinx Compatible devices (such as Modero panels) can be associated for use with a single Master. Each Modero panel comes with a defaulted Device Number value of 10001. When using multiple panels, it can become very easy to overlook the need to assign different Device Number values to each panel. • Press and hold the grey Front Setup Access button for 3 seconds to open the Setup page. • Press the **Protected Setup** button (located on the lower-left of the panel page), enter ***1988*** into the on-screen Keypad's password field, and press **Done** when finished. • Enter a Device Number value for the panel into the Device Number Keypad. *The default is 10001 and the range is from 1 - 32000*.
After downloading a panel file or firmware to a G4 device, the panel behaves strangely.	Symptoms include: • Having to repeat the download. • Inability to make further downloads to the panel. May get "directory" errors, "graphics hierarchy" errors, etc.… indicating problems with the Compact Flash. • Panel will not boot, or gets stuck on "AMX" splash screen. • Other problems also started after downloading to a new panel or a panel with a TPD4 file that takes up a considerable amount of the available Compact Flash. Cause: • If the G4 device already contains a large enough file, subsequent downloads will take up more space than is available and could often corrupt the Compact Flash. The demo file that typically ships with G4 panels is one such file. Solution: • DO NOT download TPD4 files (of large size) over the demo pages, or any other large TPD4 file. • First download a small blank one page file to the G4 panel using the Normal Transfer option to send/download the page. Reboot the device, then do your regular file or firmware download.

It's Your World - Take Control™

3000 RESEARCH DRIVE, RICHARDSON, TX 75082 USA • 800.222.0193 • 469.624.8000 • 469-624-7153 fax • 800.932.6993 technical support • www.amx.com